INNOPAY

Book of Insights 2021

January 2021

#EverythingTransaction

innopay.com

Foreword

Dear reader,

In this Book of Insights, you will find a compilation of INNOPAY articles about Data Sharing, Digital Identity and Payments published during 2020. For extra convenience, they are grouped together by format: blogs, interviews, podcasts and videos.

We hope you will find this useful in understanding and embracing the full opportunities of the digital era. Happy reading!

The INNOPAY team

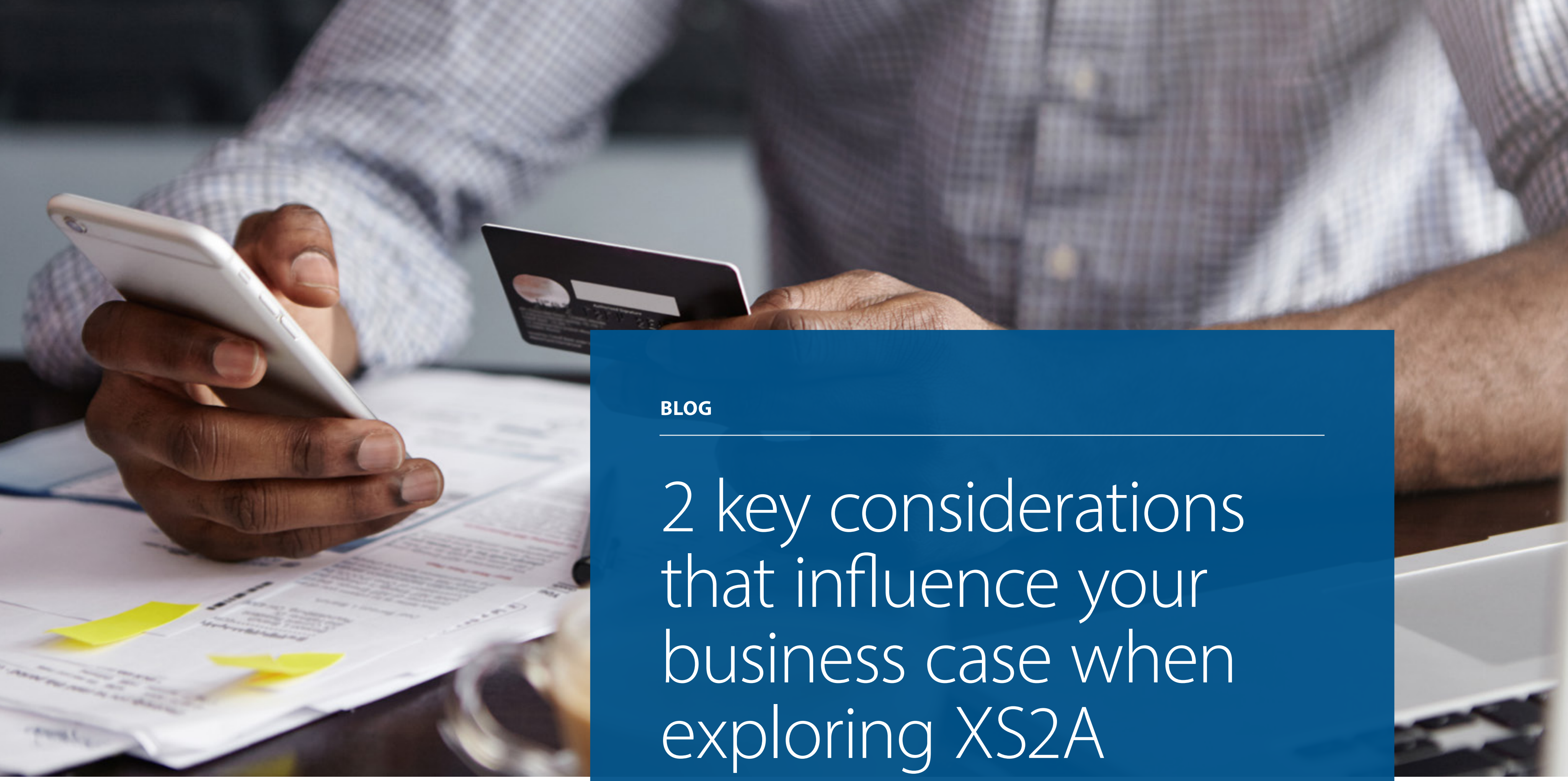
Table of Contents

Blogs

Interviews

Podcast

Videos



BLOG

2 key considerations that influence your business case when exploring XS2A opportunities

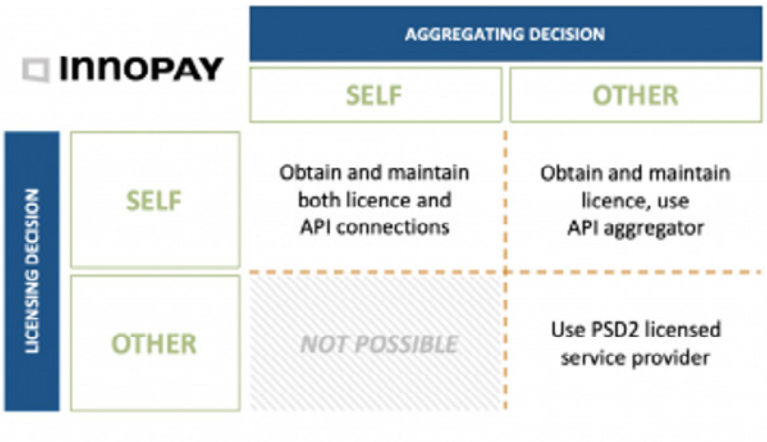
8 January 2020

Luc van Oorschot

Krijn Reijnders

PSD2 has created new possibilities for innovation within the European payments market that extend beyond the financial sector. A broad range of players, with or without a payments background, can leverage the opportunities of this legislation. Such players face two key decisions. Firstly, they must choose whether to obtain a PSD2 licence themselves or re-use a licence from a licenced service provider. Secondly, if they choose to obtain and maintain a licence themselves, they'll have to decide how to connect to banks to access the data and functionality that banks are obliged to open up: either by building and maintaining their own API connections or by using an API aggregation service provider.

For both key decisions, it is not always clear what degree of effort the options entail and what the relevant considerations are. We have explored the challenge of obtaining a licence in a previous blog. In this blog, we examine the most important criteria that are relevant in these decisions and the considerations that come with these criteria. We'll first explore the licensing decision before moving on to the decision on API aggregation.

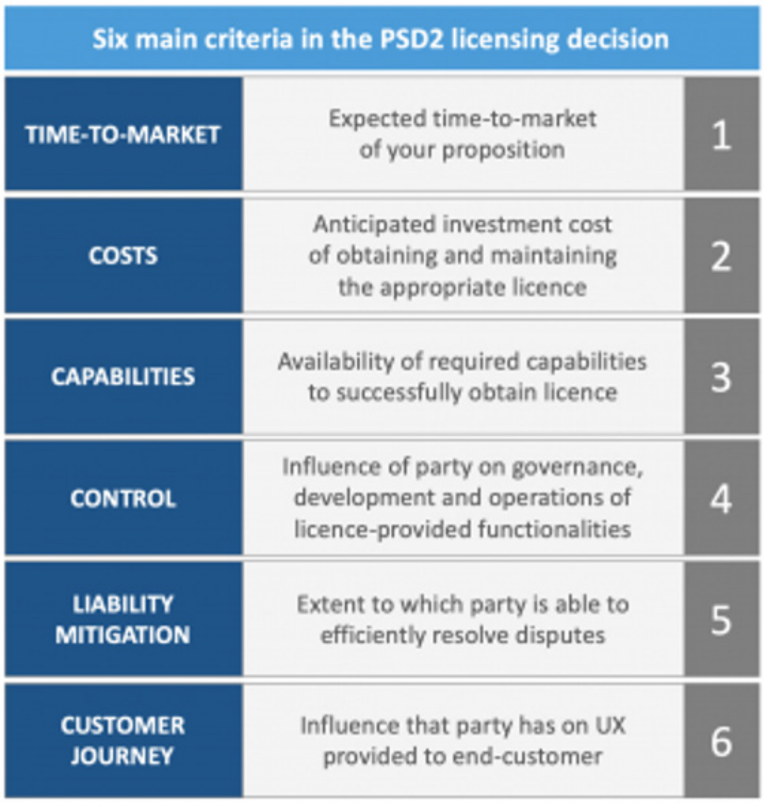


		AGGREGATING DECISION	
		SELF	OTHER
LICENSING DECISION	SELF	Obtain and maintain both licence and API connections	Obtain and maintain licence, use API aggregator
	OTHER	NOT POSSIBLE	Use PSD2 licensed service provider

Figure 1: Decision matrix for PSD2 licensing

The decision to obtain a PSD2 licence relies on six criteria

For licensing, the organisation has to make the following decision: either obtain and maintain its own PSD2 licence or re-use a licence from a licenced service provider. We have identified six main criteria that influence this decision-making process:



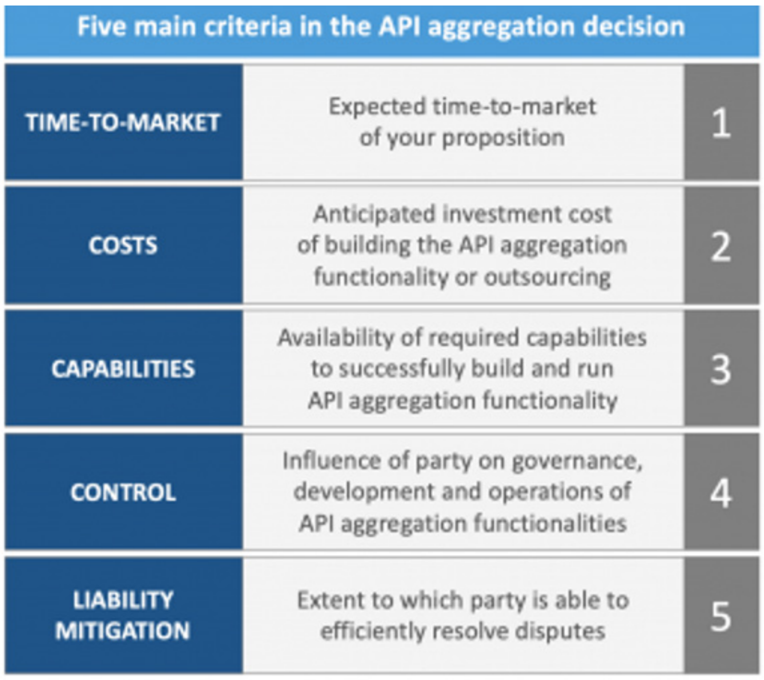
Six main criteria in the PSD2 licensing decision		
TIME-TO-MARKET	Expected time-to-market of your proposition	1
COSTS	Anticipated investment cost of obtaining and maintaining the appropriate licence	2
CAPABILITIES	Availability of required capabilities to successfully obtain licence	3
CONTROL	Influence of party on governance, development and operations of licence-provided functionalities	4
LIABILITY MITIGATION	Extent to which party is able to efficiently resolve disputes	5
CUSTOMER JOURNEY	Influence that party has on UX provided to end-customer	6

Figure 2: Six main criteria in the PSD2 licensing decision

1. Time-to-market is key in many propositions. Getting a PSD2 licence can be a time-consuming exercise, whereas a licensed service provider can provide you with PSD2 services the very next day. If you need to market a proposition quickly, a licensed service provider will enable you to do so.
2. Obtaining the appropriate licence will take time and effort and may therefore be costly in comparison to using a licensed service provider.
3. Besides costs, obtaining and maintaining a licence requires capabilities in licensing and regulations that may not always be readily available within your organisation.
4. One of the benefits of having your own licence is the control you have over the functionalities you need for your business case. A licensed service provider may not provide the flexibility in governance, development and operations that your organisation requires for a successful proposition.
5. Having your own licence also reduces complexity in liability mitigation, as involving more parties in your customer service implies additional legal frameworks and lengthier processes to resolve disputes.
6. Lastly, using a licensed service provider also has an impact on the customer journey, as under PSD2 the user provides consent to the licensed party in the bank environment. Seeing the unfamiliar name of a licensed service provider instead of your organisation's name may cause confusion among consumers and even distrust in your services.

The decision to use an API aggregation service provider depends on five criteria

If you have chosen to obtain a PSD2 licence, you will then have to decide on how to connect to the banks' APIs. In the case of API aggregation, you will need to make the following decision: either build and maintain your own API connections to banks, or source API aggregation services from a technical service provider. Please note that if you have decided not to obtain a licence, you will not be able to connect to the banks' PSD2 APIs as there is no licence to base the access on. We have identified five main criteria that influence the API aggregation decision:



Five main criteria in the API aggregation decision		
TIME-TO-MARKET	Expected time-to-market of your proposition	1
COSTS	Anticipated investment cost of building the API aggregation functionality or outsourcing	2
CAPABILITIES	Availability of required capabilities to successfully build and run API aggregation functionality	3
CONTROL	Influence of party on governance, development and operations of API aggregation functionalities	4
LIABILITY MITIGATION	Extent to which party is able to efficiently resolve disputes	5

Figure 3: Five main criteria in the API aggregation decision

1. Due to the low level of standardisation between banks' APIs, building and maintaining connections will involve a significant amount of time and effort. Using an external service provider to aggregate the API connections to banks can reduce the time-to-market of your proposition.
2. Given the focus and scale of external service providers, costs

are expected to be lower using an external service provider.

3. Besides time and effort, obtaining and maintaining the necessary API connections requires specific technical capabilities. The degree to which these are present differs per organisation.
4. Control is one of the main benefits of connecting to banks' PSD2 APIs yourself. An external service provider may not provide the flexibility in data, development and operations that is required for the success of your proposition.
5. Besides control, connecting to PSD2 APIs yourself reduces complexity in liability mitigation, as including more parties in your service offering implies (extensive) legal contracts and indirect customer interaction.

INNOPAY can help you with your business case

The possibilities of PSD2 are increasingly being explored by new players outside of the traditional financial market. INNOPAY can help you gain insights into the key decisions on which your PSD2 XS2A business case relies.

INNOPAY has extensive cross-sectoral experience in enabling organisations to reap the full potential of the opportunities opened up by PSD2. Our consulting services range from defining PSD2 strategies and identifying actionable opportunities, to assisting organisations with obtaining their PSD2 licence and selecting the most suitable API aggregation provider.

Disclaimer: Ultimately it is up to the National Competent Authority to decide whether exemptions on a technical service provider apply and there can be different opinions between NCAs and the European Banking Authority. This article reflects our expert view on the current overall applicable regulatory interpretations, but any advice on the applicable regulatory scope requires a case-by-case analysis.

Authors

Luc van Oorschot and Krijn Reijnders

ORIGINAL BLOG

GET IN TOUCH

BLOG

Future-proofing FinTech operating models: EU regulatory benchmark

7 February 2020

Josje Fiolet

Tycho van Ewijk

In the past decade, FinTech players have emerged that operate across borders with agile and customer centric propositions whilst continuously challenging the status quo. As part of their growth path, a regulatory authorisation often becomes necessary to broaden and scale up their business operations. Supervisory procedures are not always transparent, which is why this article aims to shed some light on how aspiring payment and electronic money service providers can define the best authorisation strategy. Recent INNOPAY study of authorisation procedures across Europe will support executive decision making regarding the regulatory approach. In conclusion, we explain why a Compliant by Design operating model should be on every FinTech company's strategic agenda.

Rise of FinTech and authorisations

FinTech firms that expand their business by providing financial services such as payment and electronic money services often require a regulatory authorisation (i.e. licence or registration). Becoming authorised not only future-proofs the sustainable growth of the business, but also signals trustworthiness towards market participants such as consumers and other financial institutions.

Statistics show that the number of authorised payment and electronic money institutions in the EU is growing at a staggering rate: from 248 to 1,311 (January 2017 to January 2020), which is an increase of 529%.[1] Main growth drivers are new licences for third-party providers under the Payment Services Directive 2 (PSD2), the diversifying financial ecosystem with new (tech) companies starting to offer regulated services, and Brexit which is forcing financial institutions to obtain additional authorisations to retain market access.

New insights in European authorisation procedures

Acquiring an authorisation can be complex and costly, because internal procedures need to be (re)designed in line with the applicable requirements and the exact requirements are often unclear upfront. Therefore, it is important for FinTech firms to develop an optimal authorisation strategy. One of the first steps is to decide in which country to apply for the authorisation. The right choice depends on criteria including the supervisory approach and the regulator's level of transparency. These criteria can be assessed by comparing the availability and quality of information on authorisation procedures in various countries.[2] Therefore, INNOPAY assessed the authorisation procedures in 13 countries as the basis for helping FinTech firms to determine their optimal authorisation strategy.

The 13 European supervisors that were selected for the benchmark have issued 82% of the payment licences and 88% of the electronic money institution licences between them, so this can be regarded as a representative sample. To study best practices in transparency and proactiveness, the aim was to identify the supervisors that provide the most successful and efficient support to FinTech firms during the authorisation process. Therefore, the supervisors were evaluated on the following related topics: (i) the availability and quality of relevant information, and (ii) the accessibility of and required effort for the authorisation procedure (see Figure 1).

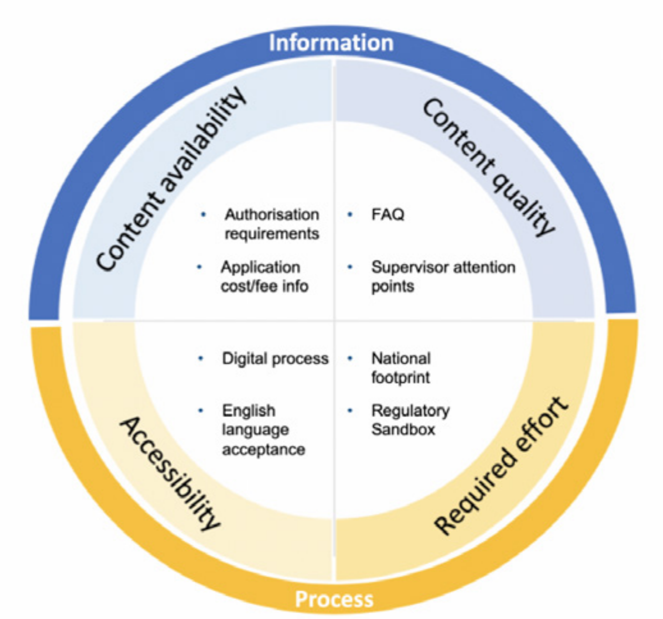


Figure 1: Key criteria used for evaluation of supervisory authorisation procedures. © INNOPAY. All rights reserved.

Key findings

The results of the study of the authorisation procedures in the 13 countries reveal that the level of transparency and proactiveness varies greatly among the financial authorities analysed.

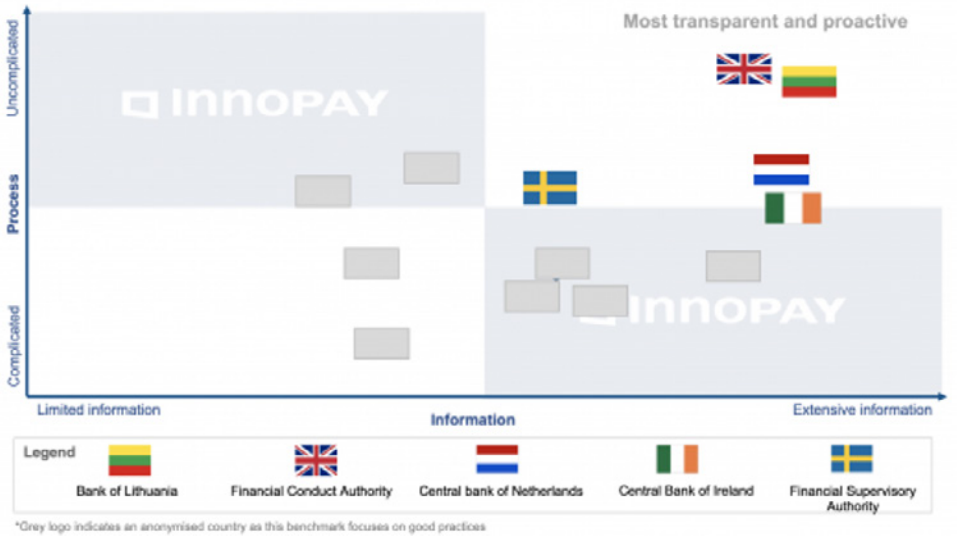


Figure 2: Relative position of different supervisors across Information and Process axes, based on INNOPAY analysis. © INNOPAY. All rights reserved.

The top-right quadrant shows the supervisors with the highest perceived level of transparency and proactiveness: Republic of Ireland, Lithuania, the Netherlands, Sweden and the United Kingdom (UK). The positive results of these countries are mainly due to the following reasons:

- Ireland provides detailed local authorisation requirements. Interestingly, Ireland is the only country without initial authorisation fees, although all regulated firms do need to pay yearly supervisory costs (just as in other countries);
- Lithuania sets itself apart by providing clear information such as FAQs and tutorial videos, in conjunction with more relaxed local requirements such as no need to pay regulatory fines in the first year after authorisation;
- The Netherlands excels in terms of the availability and quality of published information such as authorisation manuals in both Dutch and English, and due to having a digital portal for the authorisation applications;
- Sweden excels in providing extensive 'what' and 'how to' information for applicants via a handbook, clear template application forms and additional explanatory notes;
- The UK optimises both the Information and Process aspects by not only providing transparent and high-quality information, but also by having a straightforward and understandable process and stimulating FinTech through clear regulatory sandbox procedures with actual FinTech use cases.

Regulatory approach towards FinTech firms

Regulators often promote the fact that they foster innovation, but many FinTech firms wonder what that means in practice. To clarify this, the INNOPAY study additionally looked into the regulatory approach towards FinTech firms. The findings were largely positive; various regulators publish research on FinTech activities and support FinTech firms through initiatives such as regulatory sandboxes and innovation hubs (see Figure 3).

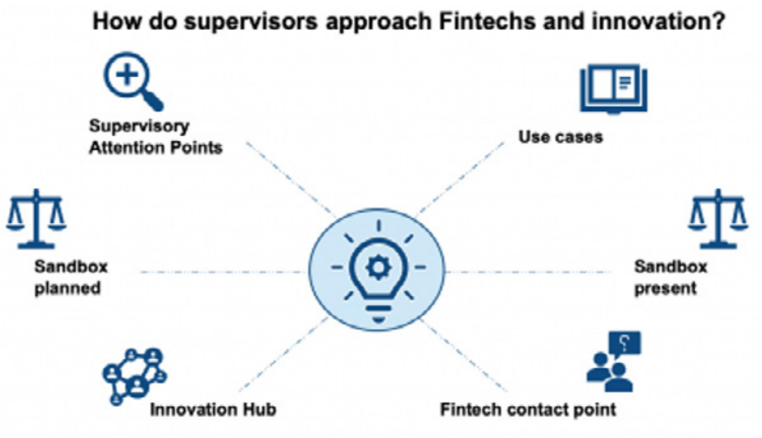

How do supervisors approach Fintechs and innovation?
Supervisory Attention Points
Use cases
Sandbox planned
Sandbox present
Innovation Hub
Fintech contact point

Figure 3: Examples of Fintech support procedures by regulators in EU.
© INNOPAY. All rights reserved.

Three examples of proactive countries

- UK: FinTech firms can test their innovative products and services in a regulatory sandbox. In fact, the FCA chairs the Global Financial Innovation Network, which is a cross-border regulatory sandbox comprising 29 regulatory bodies around the world.
- France: in July 2019, the ACPR announced its plans to create a voluntary framework for crypto firms including capital requirements, tax mandates and consumer protection protocols.
- Germany: the legislator and supervisor are reacting to FinTech developments by proactively establishing new (authorisation) regulations around crypto assets such as utility, investment and payment tokens.[3]

Claims by supervisors that they facilitate innovation and competition can create an expectation that they apply 'more relaxed' or 'FinTech-friendly' procedures for innovative firms. However, the study reveals that regulatory requirements are almost never loosened, meaning that FinTech firms must ensure a compliant operating model regardless of their chosen home country.

Why compliance by design should be on every strategic agenda

Based on 20 years of digital transformation and innovation experience, INNOPAY believes that the fast pace of digital change will only accelerate further as everything increasingly becomes a transaction. To control this new data-driven world, almost all existing rules and regulations will need to be adapted or updated. This will further intensify the current compliance and operational risk burden. Supported by the findings from the INNOPAY benchmark study, we are convinced that companies with a Compliant by Design operating model will consistently outperform FinTech companies that lack such a model. The latter will have to deal with a much greater degree of change, higher implementation and operational costs and inherent risks. History has shown that shareholders are rarely kind to such organisations, especially when the expanding cost base does not create any top-line growth value. Therefore, every executive board in the FinTech sector should ensure that restructuring the operating model – including developing an authorisation strategy – is on their company's strategic agenda and roadmap.

With our expertise in FinTech, payments and financial authorisations, INNOPAY can provide support with all the challenges to be tackled on the way to obtaining an authorisation and ensuring compliancy by design. We do so by (re)designing an effective and compliant operating model that suits your company's strategy, whilst aligning as much as possible with the current way of working. To further discuss your own case and how we can help you, do not hesitate to contact Josje Fiolet.

[1] EBA Public Register, https://euclid.eba.europa.eu/register/pir/search

[2] In every country the same financial authority is responsible for licensing payment institutions and electronic money institutions, which makes sense as both financial institution types provide payment services

[3] Changes in the German Banking Act (Kreditwesengesetz, KWG) will enter into force on 1 January 2020, as transposition of AMLD5, resulting in crypto assets qualifying as financial instruments. This results in a KWG-licence as bank or investment firm at BaFin.

Authors

Josje Fiolet and Tycho van Ewijk

ORIGINAL BLOG

GET IN TOUCH

BLOG

The EU Data Strategy: the data equivalent of GSM at last?

26 February 2020

Douwe Lycklama

Last week's publication of the European Union's data strategy should be seen as a landmark event. It lays the foundations for finally moving towards a different digital economy based on a level playing field for data. As such, it has the potential to become the data equivalent of GSM.

Under the new strategy, companies and citizens will have not only legal but also functional control of their data, and will be able to re-use their data elsewhere. This reduces the natural lock-in currently exploited by platform providers, meaning that powerful monopolistic positions will no longer be a given based on size alone. With its Bluesky initiative, Twitter is already anticipating this change by shifting from platform to protocol and web inventor Tim Berners-Lee is pursuing a similar object with the Solid project.

Just as we have increasingly found ways to minimise industrial pollution over the past century, we now have to reduce 'data pollution' by creating a decentralised, public/privately governed and secure infrastructure for the free movement of this important asset – an infrastructure which is the sum of separate (legal, operational, functional) yet interoperable platforms.

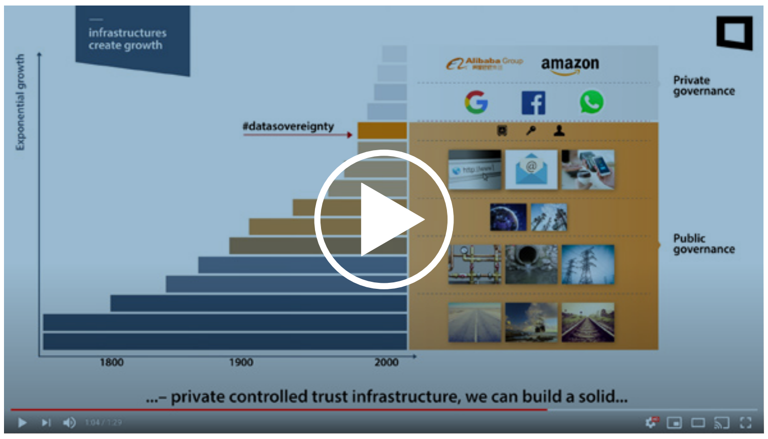
At INNOPAY we fully endorse this move as we believe it creates opportunities for businesses, sectors and nations to accelerate their role in the digital economy.

Businesses now have to review the way they operate in the increasingly digital ecosystem. How can connectivity barriers be reduced? How can they build trust while trading digitally? How can they leverage data assets across the whole value chain, while remaining in control?

Bundling digital requirements, challenges and experience, centred around common needs, can give individual industries (such as automotive, chemicals or agriculture) an edge. How can companies within those sectors harmonise data-sharing practices in order to optimally benefit from the level playing field for data while reducing connectivity costs and fragmentation?

Countries have the opportunity to structure their own digital economies to reduce their dependency on large, privately held platform players. Focusing on cross-sector interoperability of data exchange will improve the chances of success for new initiatives, as they will be able to benefit from countless potential new customers whose data is no longer locked in. Vibrant digital ecosystems can grow on such foundation.

In the 1980s, the EU redefined the global telecom industry by introducing the Global System for Mobile Communications (GSM) – a decentralised paradigm with standards, governance and adherence obligations. Something which we call ‘Afsprakenstelsel’ in Dutch’. This allowed a worldwide ecosystem of telecom providers to develop without compromising on the end-user service in terms of reach and data portability. Nowadays, it is possible to change providers without losing your data (i.e. your personal mobile number): a real-life example of data sovereignty before the term had even been coined. At INNOPAY, we believe that today’s EU Data Strategy forms the perfect foundation for the data equivalent of GSM.



...– private controlled trust infrastructure, we can build a solid...

Video: Infrastructure creates growth

Author

Douwe Lycklama

ORIGINAL BLOG

GET IN TOUCH

BLOG

Dealing with data in the context of COVID-19: A call for data sovereignty

9 April 2020

Mariane ter Veen

These are unprecedented times, and the current coronavirus (COVID-19) pandemic raises some essential questions in the data debate. Governments worldwide are faced with the challenge of gathering the right data so they can track cases and fight the spread of the coronavirus. Their solutions generally lie in one of two directions*: totalitarian surveillance or citizen empowerment. From our perspective, the solution is crystal clear. At INNOPAY, we are strong advocates of enabling organisations and individuals to manage access to their data in effective and empowering ways. This is urgently needed to build the necessary trust so that data owners will provide consent. Data-sharing based on consent is vital to keep the digital transactions ecosystem well-oiled... and it is also crucial in the fight against COVID-19.

Data as the new fabric of society

Data is rapidly becoming the new fabric of society, and we still need to explore all of its facets. Data – including personal data, access and authorisation rights, obligations, attention and reputation – represents value and forms the basis of new business models. This is part of what we call the 'transactional phase' of the internet, which has as-yet-untapped value potential. Now, the challenge is to find ways to better understand this new currency and its impact as the basis for making the right decisions – both as individuals and as organisations.

When talking about data, I sometimes feel we are like the Inuit; they have dozens of words for 'snow'. We need more words to clarify what we mean: a new data dictionary. So, let's introduce some new terminology.

Data? It's all about access

Everybody seems to be talking about data – from the 'cool stuff' you can do with data (applications such as blockchain, artificial intelligence (AI) and 'big data'), to data itself: data quality, data sharing, data leaks and data security. But it strikes me that there's a gaping hole in all these conversations: access to data. At INNOPAY we believe that data availability and data access are preconditions for any data application, and we have expressed this in our Triple A Model (See Figure 1). As we increasingly move towards the transactional era, this apparent collective lack of interest in managing data access is starting to cause serious problems.

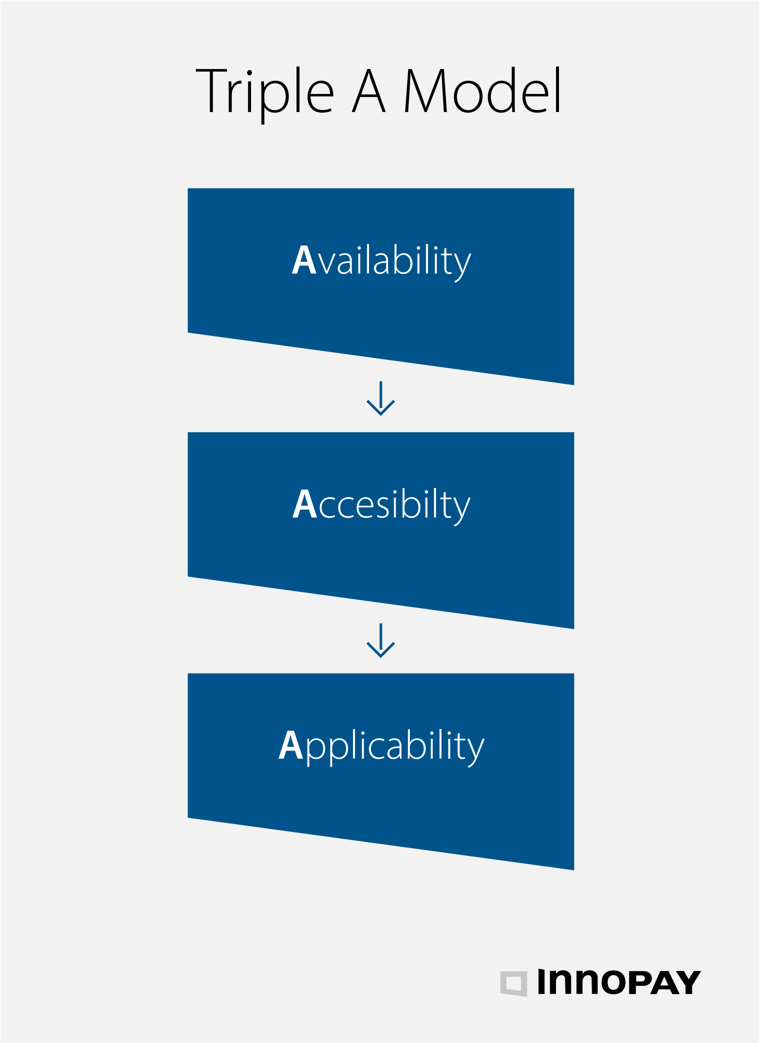


Figure 1: The Triple A Model, data availability and data accesibility are prerequisites for any application

Most people haven't tended to care about data access and have so far been sharing their data willingly. Many regard it as 'a price you have to pay'; if you want to stay connected through social media and want the convenience of ordering online, you simply go ahead and click on "I agree". However, people are becoming increasingly aware of the fact that they subsequently have no control over the data they provide and that ultimately 'they are the product' themselves.

The realisation is slowly dawning that data is in the hands of a few. Tech giants such as Facebook, Google, Amazon and so on are using people's data for their own benefit, yet giving nothing (or very little) in return. Besides that, this leaves large groups of people open to undesired and often imperceptible influencing and numerous privacy issues. Video communication platform Zoom suffered a high-profile privacy breach just last week, for example. So, people are slowly beginning to question the situation: 'Is this the way I want my data to be dealt with? Isn't it my data? And shouldn't I benefit from it?' But up until now, the only choice they have is to take negative action, such as deciding to leave Facebook or refusing to share their data... and no longer being able to make use of certain services as a result.

Data sovereignty offers an alternative

In times of crisis, such as the current fight against COVID-19, a common governmental reflex is to think in terms of regulation and force. And citizens tend to agree to whatever is necessary in order to contain the situation. A similar thing happened right after 9/11, for example, when most people accepted that there was a legitimate need for the US federal government to create a veneer of legality for a flagrantly illegal dragnet telephony data mass surveillance programme under the US Patriot Act. The danger lies in the fact that today's 'crisis' measures are tomorrow's 'normal'. Luckily there is an alternative. That alternative is based on a positive approach; it is based on restoring trust by giving people the tools to manage their own data. Let me give you an example of how important it is to organise trust and make data sovereignty part of the design principles of any data application.

Coronavirus apps

The OLVG Hospital in the Netherlands has taken the initiative of developing a free and easy-to-use app so that people can input and monitor their data themselves. It provides complete transparency and openness about how the data provided will be used. This builds the necessary trust to encourage people to submit their data. The hospital then monitors that data and calls individuals whenever it is considered necessary.
The overwhelming adoption of the app and the quality of the data entered is proof that this approach is successful. People's reactions on social media telling others about the caring personal calls they have received, are further evidence that trust boosts adoption. Ultimately, these kinds of apps could prove to be very useful tools (not least thanks to the higher-quality data!) in the fight against coronavirus, and perhaps even more useful than mass surveillance by the tracking and tracing of smartphones.

The foundation of guaranteeing access to data: trust, trust and trust

Governments around the world should not fight the pandemic at the expense of basic human rights – at the expense of citizens' control over their own data. That's why we welcome the European Commission's Recommendation of 9 April on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis. Policymakers should choose the right direction and push for data sovereignty as the central design principle in all processes and applications using data. Similarly, organisations should enable their customers to manage their own data in terms of who may access it and under what conditions. They can do so by offering them transparency and by providing them with the necessary tools, such as dashboards to control the use of their data. This will build trust, and this trust is the essential foundation for encouraging everyone to provide consent so that their data can be shared seamlessly. And seamless data sharing is vital to keep the digital transactions ecosystem well-oiled, and vital in the fight against COVID-19.

* Financial Times, Harari, 2020
https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Author
Mariane ter Veen

ORIGINAL BLOG

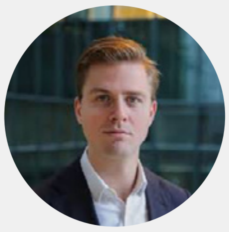
GET IN TOUCH

BLOG

Analysis: How the EU sets out guiding principles on privacy and security for use in development of contact-tracing app

24 April 2020

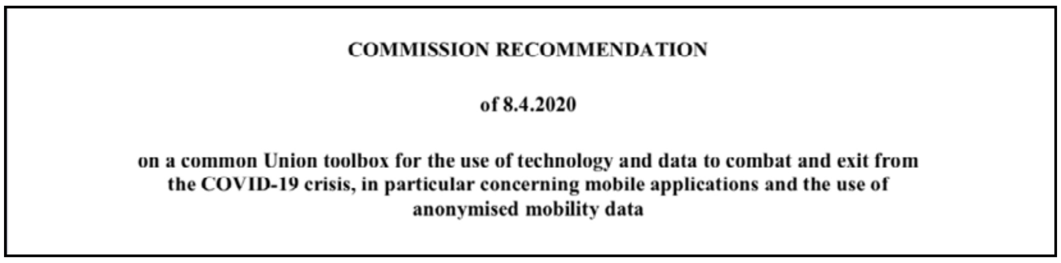
Mariane ter Veen



Jim de Wolf

Comparing the Dutch Veilig Tegen Corona coalition's ten criteria against the EU Recommendation on a common toolbox for the use of technology and data to combat and exit from the COVID-19 crisis

The development of contact-tracing applications ('apps') to combat COVID-19 is under close scrutiny. Veilig Tegen Corona (VTC), a coalition of concerned groups in the Netherlands, has published a list of ten key criteria such an app should meet. Meanwhile, on 8 April 2020, the European Commission issued its Recommendation to all Member States on creating a common European Union (EU) toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.[1]

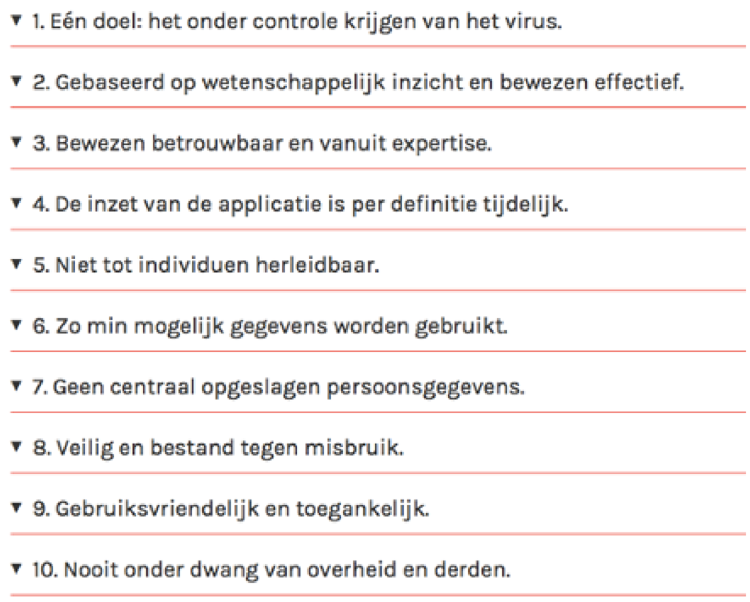


COMMISSION RECOMMENDATION

of 8.4.2020

on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data

INNOPAY has compared the VTC's ten criteria against the EU Recommendation to analyse the extent to which the Recommendation addresses the valid concerns of the VTC coalition and other pressure groups.



▾ 1. Eén doel: het onder controle krijgen van het virus.

▾ 2. Gebaseerd op wetenschappelijk inzicht en bewezen effectief.

▾ 3. Bewezen betrouwbaar en vanuit expertise.

▾ 4. De inzet van de applicatie is per definitie tijdelijk.

▾ 5. Niet tot individuen herleidbaar.

▾ 6. Zo min mogelijk gegevens worden gebruikt.

▾ 7. Geen centraal opgeslagen persoonsgegevens.

▾ 8. Veilig en bestand tegen misbruik.

▾ 9. Gebruiksvriendelijk en toegankelijk.

▾ 10. Nooit onder dwang van overheid en derden.

Figure 2: VTC's 10 criteria

1. One purpose: getting COVID-19 under control

This demand of the VTC coalition deals with the development and introduction of the contact-tracing app. It should have one single goal: getting the virus under control.
The Recommendation takes the same stance. Possessing of data of natural persons is subjected to Regulation (EU) 2016/679). Consideration 8 reminds us that in any case, the purposes and means of the data processing, what data are to be processed and by whom, should be clear and specific.[2] Besides that, the Recommendation describes the privacy and data protection aspects of the use of mobile applications. Particularly, one of the principles that must be observed is to "strictly limit the processing of personal data for the purposes of combating the COVID-19 crisis and ensure that the personal data are not used for any other purposes such as law enforcement or commercial purposes".[3] Furthermore, regarding the use of mobility data to inform measures and the exit strategy, it specifically indicates that "the second priority for the toolbox should be a common approach for the use of anonymised and aggregated mobility data necessary for: (1) modelling to map and predict the diffusion of the disease and the impact on needs in the health systems in Member States, such as, but not limited, to Intensive Care Units in Hospitals and Personal Protective Equipment; and (2) optimising the effectiveness of measures to contain the diffusion of the COVID-19 virus and to address its effects, including confinement (and de-confinement), and to obtain and use those data".[4] Finally, the Recommendation also expressly excludes sharing of the data with third parties.[5]

2. Based on scientific insight and proven effectiveness

Here the VTC coalition expresses the expectation that the contact-tracing app should be based on scientific results and be demonstrably effective.

Throughout the Recommendation, is it clear that this is paramount for the European Commission too. One of the principles of the toolbox is the preference to opt for the least intrusive yet most effective measures. Besides that, Member States are strongly encouraged to exchange best practices on the use of mobility data, share and compare modelling and predictions of the diffusion of the virus, and monitor the impact of measures to limit its diffusion.[6]

3. Proven reliability and based on expertise

This third point is an extension of the second one and states that the application should be developed based on expertise and its reliability should be proven.

The Recommendation states that the toolbox should be shared with the European Union's international partners to exchange best practices and help address the spread of the virus worldwide. The principles with regard to the mobile warning and prevention application should also take into account technical requirements concerning appropriate technologies to ensure secure and reliable device proximity, encryption, data security, storage of data on the mobile device, possible access by health authorities and data storage.[7]

4. Usage of the application is temporary

The VTC collation calls for the app to be purely intended as a temporary solution.

This is expressly covered by the Recommendation insofar as the principles for the contact-tracing application cover the expiration of measures taken and the deletion of personal data obtained through these measures when the pandemic is declared to be under control at the latest, and that the deletion of data should in principle take place after a period of 90 days or when the pandemic is declared under control.[8]

5. Not traceable to individuals

In order to prevent potential stigmatisation and targeted abuse, the coalition argues that it should never be possible to trace information gained from any data gathered back to an individual.

The European Commission takes the same view; no fewer than six paragraphs of the Recommendation are devoted to this topic.[9] The Recommendation not only requires anonymity, but also adds to this demand by explicitly requiring safeguards to prevent de-anonymisation and avoid reidentification of individuals, including guarantees of adequate levels of data and IT security and assessment of reidentification risks when correlating the anonymised data with other data.

6. Usage of as little data as possible

The VTC demands that as little data as possible should be required from users.

The European Commission reflects on this aspect in the considerations. Existing EU law permits data collection only in narrowly defined circumstances or on the basis of consent of the user or subscriber. Only after having been provided with clear and comprehensive information to traffic and location data, the storing of information and the gaining of access to information stored in the terminal equipment, such as a mobile device, of a user or subscriber. The EU upholds the principle of data minimisation. This is set out in consideration 25, which stipulates that public health authorities and research institutions should process personal data only where adequate, relevant and limited to what is necessary, and should apply appropriate safeguards such as pseudonymisation, aggregation, encryption and decentralisation.[10]

7. No central storage of personal data

The VTC opposes the central storage of personal data.

This is not explicitly covered by the Recommendation. The European Commission upholds the principle of data minimisation, of course, and points out the requirements of integrated data protection and privacy-by-design principles, but this does not automatically translate into the prohibition of central storage of data.[11]

8. Secure and abuse-resistant

The VTC demands data security, including adequate measures against abuse.

Consideration 17 of the Recommendation pays attention to the protection of fundamental rights and respect for private and family life. Article 16(4) instigates the guiding principle of effective cybersecurity requirements to protect the availability, authenticity, integrity and confidentiality of data to be processed in the contact-tracing app.[12]

9. User-friendly and accessible

For effective use of the application, it is essential that the user base is as wide as possible, which is why this ninth point emphasises the importance of user-friendliness and accessibility.

The Recommendation agrees that transparency and clear and regular communication are paramount to ensure public trust and that the European e-Health systems and services should work with interoperable applications, to achieve a high level of trust and security, enhance continuity of care and ensure access to safe and high-quality healthcare. Transparency requirements on the privacy settings will help to address these considerations and ensure trust in the applications.[13]

10. Never enforced by governments or third parties

Lastly, VTC demands that the contact-tracing application cannot be thrust upon the population by governments or third parties.

This demand is partly covered by the Recommendation in the sense that the use of the application should always require consent and the protection of natural persons with regard to the processing of personal data and the free movement of such data. Besides that, the Recommendation contains a requirement to strictly limit the processing of personal data to the purposes of combating the COVID-19 crisis and to ensure that the personal data are not used for any other purposes such as law enforcement or commercial purposes.[14]

Concluding remarks

It can be concluded that the EU Recommendation addresses many of the concerns expressed by the coalition, since it already covers nine out of the ten criteria. The Recommendation therefore serves as an excellent starting point for app developers to ensure protection of fundamental rights and freedoms, particularly the rights to privacy and protection of personal data.

It is encouraging to see how quickly the European Commission has reacted to the various market tendencies and government activities to develop mobile applications based on the use of anonymised mobility data to combat COVID-19. It is of the utmost importance to critically monitor the actions of governments and institutions and to validate every step in developing and rolling out a contact-tracing app in the battle against COVID-19. The ability to fall back on established rules to protect fundamental rights within the EU will help to ensure the security of personal data, both now and in the future.

[1] A European Recommendation is an instrument that does not possess any legal force but is negotiated and voted on by Member States and has political weight insofar as it is an instrument of indirect action aiming at preparation of legislation in Member States. It differs from a Directive only by the absence of obligatory power.

[2] Article 6(1)(c) or (e) and Article 9(2)(i) of Regulation (EU) 2016/679).

[3] Article 16(1) Commission Recommendation (EU) 2020/4/8.

[4] Article 18 Commission Recommendation (EU) 2020/4/8.

[5] Article 20(6) Commission Recommendation (EU) 2020/4/8.

[6] Articles 16(2) and 19 Commission Recommendation (EU) 2020/4/8.

[7] Articles 12 and 16(3) Commission Recommendation (EU) 2020/4/8.

[8] Articles 16(5) and 20(5) Commission Recommendation (EU) 2020/4/8.

[9] Articles 16(2)(6) and 20(1)(2)(3)(4) Commission Recommendation (EU) 2020/4/8.

[10] Consideration 25 and article 16(2) Commission Recommendation (EU) 2020/4/8; Directive 2002/58/EC of the European Parliament and Regulation 2016/679.

[11] Consideration 25 and article 8 Commission Recommendation (EU) 2020/4/8.

[12] Consideration 17 and article 16(4) Commission Recommendation (EU) 2020/4/8.

[13] Consideration 6, 30 and article 16(7) Commission Recommendation (EU) 2020/4/8.

[14] Consideration 7 and article 10(1) Commission Recommendation (EU) 2020/4/8.

Authors

Mariane ter Veen and Jim de Wolf

ORIGINAL BLOG

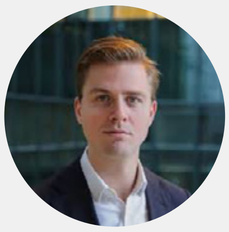
GET IN TOUCH

BLOG

Data sovereignty holds the key to widespread adoption of COVID-19 apps

26 December 2020

Mariane ter Veen



Jim de Wolf

Concerns are growing as ever-more governments explore the idea of tracking and tracing apps as a way of monitoring and slowing the spread of COVID-19. Obviously, society must use all possible means to fight the pandemic, including technology and data. But that shouldn't mean casting aside the fundamental European values. Numerous institutions, associations, interest groups and experts have already expressed their reservations and are calling for a more rigorous app development process to ensure that those values are upheld. But what do they mean? What are 'European values'? And how can we safeguard them?

Data as the new fabric of society

Due to the COVID-19 crisis, a variety of mobile applications are being developed in different countries, many of them by governments and public authorities. The apps are aimed at using technology and data to slow the spread of coronavirus infection until a vaccine is widely available. Each app is slightly different. For example, certain apps are designed for the general public, while others are limited to closed user groups directed at monitoring contact in the workplace. However, they all tend to serve three general functions.

The key functionalities of a coronavirus app (from the European Commission Recommendation):

1. Monitoring the user's health (often combined with a self-diagnosis questionnaire), informing/advising them and facilitating the organisation of medical follow-up in the case of symptoms
2. Warning the user if they have been in proximity to an infected person and advising them on appropriate action in order to break the chain of infection. This is key in both slowing the initial spread of the virus and preventing resurgence after lockdown measures are eased
3. Monitoring and enforcing the quarantine of infected people, possibly combined with features assessing their health condition during the quarantine period.

Two main challenges: adoption and trust

Generally speaking, the effectiveness of such mobile apps has not been fully evaluated, mainly due to the pressure to launch a coronavirus app as quickly as possible. In our view, success depends above all on sufficient user penetration. This presents two main challenges: adoption and trust.

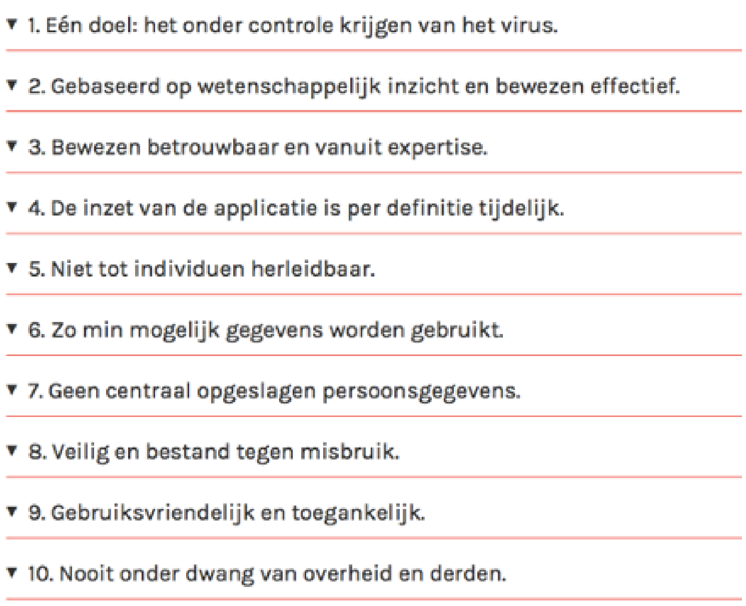
For widespread adoption, firstly a high percentage of the population must be able to 'technically adopt', i.e. they must own a mobile device and be tech-savvy enough to use it. Secondly, a high percentage of those mobile device owners must actually download the app and consent to the processing of personal data concerning them (without subsequently withdrawing that consent).

Trust is above all the most important factor in achieving adoption. Citizens must trust that their data will be protected by appropriate security measures and used exclusively for the specified goals to which users have consented. Public health authorities should not only endorse the app but must also be able to take necessary action based on the data generated by it. This requires integration and data sharing with other systems and applications, and ideally also cross-border and cross-regional interoperability with other systems, which adds an extra dimension to the issue of data security and trust regarding how the data will be used.

Dealing with data in a 'European way'

Clearly, the development of a national coronavirus app requiring citizens to volunteer their data for surveillance purposes blurs the boundaries between public health and civil liberties. Therefore, in recent weeks, various European Member States, public and private-sector institutions, experts, associations, opinion makers and trendwatchers have expressed their concerns about cybersecurity, data security and privacy. There are growing calls for coordination at EU level to focus on 'European values', and especially on the protection of the fundamental right to privacy and protection of personal data.

For example, in mid-April Veilig Tegen Corona, a coalition of concerned groups in the Netherlands, called for the development process of coronavirus apps to be carefully considered and above all focused on utility and necessity. The coalition has published a list of ten key criteria for such an app.



▼ 1. Eén doel: het onder controle krijgen van het virus.

▼ 2. Gebaseerd op wetenschappelijk inzicht en bewezen effectief.

▼ 3. Bewezen betrouwbaar en vanuit expertise.

▼ 4. De inzet van de applicatie is per definitie tijdelijk.

▼ 5. Niet tot individuen herleidbaar.

▼ 6. Zo min mogelijk gegevens worden gebruikt.

▼ 7. Geen centraal opgeslagen persoonsgegevens.

▼ 8. Veilig en bestand tegen misbruik.

▼ 9. Gebruiksvriendelijk en toegankelijk.

▼ 10. Nooit onder dwang van overheid en derden.

European data strategy is built on European values
Luckily the EU already has a vision for European data sharing in place that revolves around the European values: the European Data Strategy. This was developed to ensure Europe's global competitiveness. The European Commission considers data to be an essential resource for economic growth, competitiveness, innovation, job creation and societal progress in general. (Click here to watch an interview with Yvo Volman, Head of EU Communication and Technology).

In an extension of the European Data Strategy, an EU Recommendation sets out the recommended steps and measures for developing a common EU-wide approach for the use of mobile apps and mobile data. In the context of fighting the coronavirus pandemic, this recommendation can be applied to the development and use of tracking and tracing apps with respect to fundamental European values.

Closer examination of Veilig Tegen Corona's ten criteria reveals that most of the concerns raised are addressed by the EU Recommendation's principles covering privacy and data-protection aspects of use of mobile applications. In other words, these principles serve as an excellent basis for app developers to ensure sufficient safeguards against the abuse of data generated by a national/international COVID-19 app.

(Click here for a full analysis of how the EU Recommendations cover the ten criteria).

How to safeguard European values

We welcome both the Veilig Tegen Corona criteria and the EU Recommendation because they echo our long-standing call for data sovereignty. People need ways to exercise their data rights. The importance of this had already started to emerge in the data economy before the COVID-19 outbreak, but the pandemic has now propelled the issue to the forefront of people's minds and to the top of political agendas.

Thanks to the EU Data Strategy and its Recommendation, tangible, actionable and executable guidelines are now in place to enable people and organisations alike to govern their own data, putting them in charge of deciding who has access to their data and under what conditions.

At INNOPAY, we believe that data sovereignty holds the key to the success of COVID-19 apps since it provides the foundation for widespread adoption based on user trust, in line with European values.

Author

Mariane ter Veen and Jim de Wolf

ORIGINAL BLOG

GET IN TOUCH

BLOG

Libra - A simple currency? Or a first manifestation of the transactional Internet?

28 May 2020

Shikko Nijland

Douwe Lycklama

Guest Author:
Chiel Liezenberg

This article is based on an excerpt from our award-winning book Everything Transaction, that was published in 2019. In view of the recently updated white paper on Libra and the renaming of Calibra as Novi, this part of the book is now more relevant than ever. On June 18, 2019, Facebook along with 27 founding members of the Libra Association announced their intention to introduce Libra – a simple global currency and financial infrastructure that will empower billions of people in 2020[1]. For those wondering if Libra is something to take seriously: within seven days Libra made it onto the agenda of the G7[2], another week later several US congressmen sent a letter to Facebook urging them to stop Libra[3] and within a month, Facebook was called to a congressional hearing about Libra[4]. And all that just for intending to introduce a solution. Last month Libra published the second version of its white paper, which notably reflects the result of the intensive dialog with regulators worldwide.

Libra is much more than what it appears to be

At first glance, we can now clearly recognise Libra as a middleman with a network model platform strategy, addressing a multi two-sided market with global peer-to-peer payment as a first symmetrical proposition based on institutional trust. Digging a little deeper, we could come to the conclusion that Libra addresses the two big fixes and is perhaps a first manifestation of the transactional Internet with the infrastructural trust that we so clearly foresee. So, let's take a closer look at Libra.

Libra, Novi. What is all this exactly?

Like in many initiatives of this magnitude, Libra is many things at once. To get clarity, we first have to understand the different components of Libra. To begin, there is the global digital currency Libra (abbreviation: LBR) that is backed by the Libra Reserve assets (fiat currency) to give it a stable intrinsic value. Libra is exchanged in transactions initiated through wallets, or Libra Clients. The Libra Blockchain – a programmable distributed database – stores the Libra transactions. It is powered by the Libra Protocol and the Move programming language in a first open-source implementation called Libra Core that is run by a network of permissioned participants that collectively constitute the Libra Network. Database entries are under control of end users through cryptographic keys, as used in cryptocurrencies.

A distributed database based on blockchain technology

Next, there is the independent Libra Association based in Switzerland that publishes the Libra Core, permissions the participants and will govern the Libra Network and Libra Reserve through the Libra Association Council as its governing body. Then there is the Libra Ecosystem made up of the Libra Clients (wallets), Validator Nodes (network), and Libra Developers contributing to the ecosystem in multiple ways. And finally, there is Novi (formerly known as Calibra), a Facebook subsidiary that is set up to operate independently from Facebook, that will provide the Novi Wallet app – a Libra Client to make payments in Libra[5].

How does Libra plan to break the chicken-and-egg dilemma?

Like any platform addressing a two-sided market, Libra also faces the challenge of breaking the chicken-and-egg dilemma in order to ensure mass adoption. As part of the initial announcement, Facebook mentioned 28 parties that will act as founding members of the Libra Association, some of which will also be validators within the Libra Network. These initial 28 parties consist of a mix of investment firms, technology enablers, and payment service providers, and both consumer demand and supply side service providers. Visa, Mastercard, PayPal, Uber, Booking.com, Vodafone, eBay, Spotify, Novi, and Facebook are among them. In Q4 of 2019 the ones being under financial regulation (i.a. Mastercard, PayPal, Visa) pulled out of the initiative, while the Libra initiative is being scrutinised by regulators worldwide.

With this group alone, the global distribution of Libra wallets – Novi being the most important one – to consumers for peer-to-peer payments is instantly feasible, as is the subsequent creation of acceptance points with the supply side service providers in the group. This might create the desired network effects. The incentive for tech enablers and payment service providers to be a part of this initiative is quite obvious, while the investment firms could – apart from the obvious – also be in it for the simple reason that many of their (fintech) investments would benefit hugely from Libra coming available worldwide.

Impressive founding members, with Apple, Google, Amazon, and Microsoft notably absent

It is also notable that the other big US tech platforms are not in the group. Google, Apple, Amazon, and Microsoft are likely to be fully informed, but may simply have opted to take a wait-and-see approach. However, their collective omission from this initial group could also have a more strategic angle to it: deliberately staying out for now creates the option to sway the discussion by each putting in their considerable weight at later stages, depending on the developments in regulatory response and market sentiment.

What could be the business rationale and platform strategy behind Libra?

In our book Everything Transaction we discussed the hub model and network model as the two strategic options for platform design. We also noted that big tech in the US typically opt for the hub model in combination with amassing large amounts of data. They master the scaling of single-value proposition platforms in its homogenous market to become dominant players, to then extend the value propositions and scale such platforms globally. We briefly touched on envelopment as a risk that every middleman faces, especially with single-value proposition platforms. Regardless of its size, when the core added value of a platform becomes "just a part" of an even broader proposition of a competitor, the platform becomes exposed to the risk of negative network effects. And this may just be what triggered Facebook to develop Libra.

An answer to competition on a next level

With the advent of Chinese app platforms such as WeChat that offer ultimate all-in-one convenience to consumers, including peer-to-peer, e-commerce, and in-store payments, the more specialised US-based platforms are faced with a direct threat that none of them may be able to counter individually. It is hard to imagine that any one of the US platforms—including Facebook—would allow or be allowed by others to develop an answer individually, while all of them doing this at the same time would be an obvious redundant effort and most likely be an inadequate response to such a threat.

Libra is clearly a network model platform answer to the hub model platform competition from China. It is interesting to see the US tech sector capable of such collaboration, and it may just be this jump over their own shadows that will secure their individual leading market positions in the future.

In Libra we T.R.U.S.T.?

The platform design of Libra is—knowingly or not—set up as a T.R.U.S.T. Framework as referenced in Everything Transaction. The different dimensions being clearly distinguishable. Within the Trade dimension, the Libra brand, initial value proposition, asset backing, and business model are clearly set out. The recent white paper update changed the asset backing into regular fiat currency, making Libra a (full reserve) stable coin denominated in the major currencies. In the Rules dimension, the independent Libra Association that will govern the network and reserve still has to set its final rules and criteria, but the foundation is there, and a future transition from permissioned to permission less participation has been defined. The latter has been revoked in the updated white paper of April 2020. Within the Use dimension, the initial peer-to-peer payment use case is clear while the technical specifications are clearly designed to accommodate multiple applications. In the Standards dimension, the Libra Reserve, Libra Protocol, transaction specs, Libra Blockchain specs, and Move programming language have been described, while for the Technology dimension the Internet provides the technology stack. Libra Core provides an initial implementation.

A first step toward infrastructural trust

With the Move language, developers can create Libra Clients that deploy Move modules (logic) to invoke Move resources (data) and execute transaction scripts of which the results are stored on the Libra Blockchain. With this platform design, an additional infrastructure layer is created on top of the Internet where user-controlled data is embedded and that is governed by a trust framework to create data sovereignty. These are all signs of what we refer to as infrastructural trust.

If it's just peer-to-peer payments, why are regulators and banks so concerned?

Digging into the documentation and technical specifications of Libra, there are some clear indications that Libra has been designed with a bigger play in mind. With payment as the initial application, we are inclined to view "transactions" as "payments" and consider Libra to be a payment platform, but this is misleading. There is a mention of identity as a future application, and the design of the Move language and the transaction specs allow a transaction to be any kind of exchange of data between Libra Clients that is logged on the Libra Blockchain. In addition, the Libra Protocol has a built-in charging mechanism for transactions called "gas." With gas, any data exchange within the Libra Network can be monetised. This platform design allows for a multitude of applications to be facilitated on the Libra Network in the future and makes Libra a multi two-sided platform by design.

Peer-to-peer payment is just the beginning

Libra will operate on a global scale. This implies that in order to regulate it, regulators will have to collaborate worldwide on a very short timeline to create a unified regulatory financial framework. Until now this has proven to be unattainable on any monetary topic, as the many currencies, monetary policies, banking systems, payment methods, and compliance regulations illustrate. Regulators are justly worried that they will not be able to keep up with this development (and that it may actually work), making it nearly impossible to control its roll-out and impact[6]. The Central Bank of China announced its own cryptocurrency in Q3 2019 and licenses the main financial players in its market for it[7]. Regulators and banks in the US and Europe therefore need to be particularly diligent in their response toward Libra – or the likes. This will be quite challenging, as the existing monetary system is under pressure already.

The multi-tiered bank model under pressure

As described in our book, the banking franchise and payment stack is constructed as a multi-tiered model to make the administration of the money supply scalable and manageable on behalf of the governments issuing the money. Transactions need to be authorised, cleared, and settled across all tiers. At the highest level are international banking organisations such as the Bank of International Settlements, where supra-regional and national central banks hold accounts, where in turn local banks hold accounts, where finally individuals and organisations hold accounts, where transactions are administered, and balances added up. Obviously, with the technological capabilities of the time, this was the only way to do it.

How this has changed in the last decade! Facebook proves every day that it is technically feasible to seamlessly operate a platform with over 7 billion end user accounts, held by its 2.4 billion users[8]. WeChat proves it can seamlessly process payments for its more than 1 billion active end users on a daily basis. These examples indicate that it is now technically feasible to have a single platform where every person or organisation on Earth could hold a (payment) account and make payments frictionless in a single currency—as a basic service to all of humanity.

The end of fractional reserve banking?

Another thing to consider is the amount of money involved in Libra in relation to the total amount of money in circulation. According to The Money Project[9], all money in the world totals approximately 81 trillion in US Dollar value. Of this, 28 trillion is money that can be used as a medium of exchange. All coinage and banknotes in circulation globally equal 5 trillion in US Dollar, of which 1.5 trillion is US Dollar.

In the fractional reserve banking model, not all money that is issued by a bank is backed by deposits at the bank. As a result, there is always the risk of a banking run by its customers to topple a bank. However, for individuals to create that impact is quite hard. But the balance sheets of the tech sector in the US are becoming so cash heavy, that added up this could be in the order of magnitude of a couple of trillion US Dollar. With the Libra currency, a further concentration of liquidity will result from the asset backing. If all the world's current 4.1 billion Internet users where to hold 1,000 US Dollar in Libra, this would concentrate 4.1 trillion in US Dollar value. Almost the equivalent of all coinage and banknotes in circulation worldwide.

This concentration of liquidity could give this sector a lever of some kind on the banks. Imagine a banking run of tech firms instead of consumers; this might actually be a real risk and raises the question of the effect of Libra on the global monetary system. Already, several articles point out that countries with weak currencies may be at risk in this respect[10]. Local consumers may prefer to use Libra as a currency with a stable value instead of the inflationary local currency, and further weaken the local currency.

A first manifestation of the transactional internet?

In conclusion, we have to consider that with Libra, we are witnessing the first manifestation of the transactional Internet that we so clearly see as an inevitability. In theory, the Libra platform design could provide the big fixes of breaking the trust paradox and restoring the data benefit balance that are essential to making the transactional Internet a reality.

Libra delivers on the two big fixes

Libra has clear indications of a first deliberate attempt to transition from institutional trust to infrastructural trust, embedding user-controlled data and trust in the Internet by deploying distributed ledger technology for multiple applications. It enjoys the support of an impressive group of founding members that have access to billions of consumers that stand to gain control over their data on the Libra Blockchain while they can also choose to share it with select counterparties and benefit from it in other Libra or Move applications.

There is, of course, the big reservation that the final launch implementation has yet to prove the extent to which all of this will actually be the case.

Disclaimer: Since this article was written in 2019, certain statements, claims or information may have been superseded by subsequent events or insights.

1. Libra Association. Introducing Libra: a simple global currency and financial infrastructure that can empower billions of people. (Libra Association, libra.org/en-US/wp-content/uploads/sites/23/2019/06/IntroducingLibra_en_US.pdf, June 18, 2019).
2. Reuters. France creates G7 cryptocurrency task force as Facebook's Libra unsettles governments. (Reuters, reuters.com/article/us-facebook-crypto-france/france-creating-g7-cryptocurrency-taskforce-says-central-banker-idUSKCN1TM0SO, June 22, 2019).
3. Kelly, M. House lawmakers officially ask Facebook to put Libra cryptocurrency project on hold. (TheVerge, theverge.com/2019/7/2/20680230/facebook-libra-calibra-crypto-maxine-waters-congress-regulation-investigation-halt, July 2, 2019).
4. Kelly, J. Facebook's Libra Comes Under Fire In Senate Hearing – Here's Why Congress Is Terrified. (Forbes, forbes.com/sites/jackkelly/2019/07/16/facebooks-libra-comes-under-fire-in-senate-hearing-heres-why-congress-is-terrified/#54561fff36b4, July 16, 2019).
5. Calibra. Intro. (Calibra, calibra.com, accessed in July 2019).
6. Mourdoukoutas, P. Why Big Governments And Central Banks Want To Kill Libra And Bitcoin. (Forbes, forbes.com/sites/panosmourdoukoutas/2019/07/16/why-big-governments-and-central-banks-want-to-kill-libra-and-bitcoin/#d6f071738d5f, July 16, 2019).
7. Castillo, M. del. Alibaba, Tencent, Five Others To Receive First Chinese Government Cryptocurrency. (Forbes, forbes.com/sites/michaeldelcastillo/2019/08/27/alibaba-tencent-five-others-to-recieve-first-chinese-government-cryptocurrency/#36039e031a51, August 27, 2019).
8. Statista. Number of monthly active Facebook users worldwide as of 2nd quarter 2019 (in millions). (Statista, statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/, accessed in August 2019).
9. Desjardins, J. All of the World's Money and Markets in One Visualization. (The Money Project, money.visualcapitalist.com/all-of-the-worlds-money-and-markets-in-one-visualization/?link=mktw, December 17, 2015).
10. Business Standard. Former Japan central banker warns FB's Libra may undermine monetary policy. (Business Standard, business-standard.com/article/international/former-japan-central-banker-warns-fb-s-libra-may-undermine-monetary-policy-119080200672_1.html, August 2, 2019).

Authors

Shikko Nijland, Douwe Lycklama and Chiel Liezenberg

ORIGINAL BLOG

GET IN TOUCH

BLOG

Extra boost for initiatives aimed at helping organisations to overcome their data sovereignty challenges

14 June 2020

Mariane ter Veen

Douwe Lycklama

The European Data Strategy gives extra impetus to various initiatives that are driving data sovereignty. Although many of them are in the early stages and conceptual, the first concrete use cases – and tangible results – are already emerging and the wheels of adoption are gradually starting to turn. Some of the most prominent data-sharing initiatives that drive data sovereignty include:

GAIA-X

GAIA-X is a German/French project which aims to unite cloud and edge services from European providers in a federated data infrastructure: a club of clouds whose members have to comply with a set of common rules, standards and technologies when supplying their services in order to create a level playing field from a legal, operational, technical and functional perspective.

Data sovereignty is a particular challenge for organisations in the context of the shift to cloud services as part of their digital transformation. When it comes to data sovereignty and cloud providers, legal jurisdiction is an important aspect; data is subject to the laws of the country in which it is physically stored. Therefore, data subjects may receive different levels of privacy and security protection depending on where the data centres are located. Some nations even stipulate local storage and tightly regulate whether, how and for what reasons data may be moved out of the country.

GAIA-X's goal is to create a new cloud ecosystem that will offer organisations alternatives to the currently dominant Chinese or US tech giants. Its members – which have included big-name companies and institutions such as Atos, SAP, Deutsche Telecom, Siemens and Fraunhofer from the start – may have to provide certain guarantees about data sovereignty, including data privacy, localisation and so on. The standards, rules and agreements that form the basis for GAIA-X have not yet been finalised. However, there is no doubt that the aim of GAIA-X – enabling the EU, its Member States, public and private-sector organisations and citizens to regain and maintain control over their data – will be leading in its further development. The initiators of the project plan to found their own European organisation in mid-2020.

International Data Spaces Association (IDSA)

As an international virtual network of industry and research, IDSA is actively involved in designing a trustworthy architecture for the data economy, with data sovereignty as a key design principle. It aims to facilitate the worldwide exchange of data between data providers and data users in business ecosystems in such a way that data providers stay in control of their data.

Ever since the foundation of IDSA in 2016, more than 100 companies and institutions from 20 countries and various industries, including several Fortune 500 companies, globally active medium-sized companies and software and system houses, have made progress in building the IDS architecture.

Dutch data sharing coalition

The Dutch government has been quick to realise the importance of data sovereignty for the future of the transactional internet. In 2019, the Dutch cabinet presented its vision on data sharing between companies. This ultimately led to the formation of the Dutch Data Sharing Coalition, which is aimed at stimulating decentralised cross-sectoral data sharing while ensuring that data owners maintain full control of their data. Some 25+ organisations from different industries have already signed up for the coalition.

Dutch AI Coalition

The Dutch AI Coalition (AIC) is a public-private partnership which brings together organisations representing government, business, education and society. The AIC's goal is to stimulate, support and where necessary facilitate Dutch activities related to artificial intelligence (AI). Data sovereignty is a key design principle.

Industry-specific initiatives

Additionally, various sectors are working on their own industry-specific initiatives that revolve around data sovereignty. Examples include the data-sharing schemes MedMij (Healthcare), Join Data (Agri), iSHARE (Logistics), Smart Connected Supplier Network (Manufacturing) and SBR Nexus (Finance). All these initiatives were started by public private partnerships in the Netherlands, but have since been extended to a European level.

Many of these initiatives are gaining serious traction in the market, with the first signs of adoption visible. For instance, more than 30 healthcare providers already comply with the strict requirements of the MedMij scheme.

Meanwhile, in the logistics sector, the number of iSHARE participants continues to grow steadily. One such participant is Hutchison Ports ECT Rotterdam (ECT) – one of Europe's leading container terminals – which has developed an app with a log-in system based on iSHARE identities that is used by numerous transport companies every day. As a result, ECT and its customers can share data more easily and securely than before.

And in the manufacturing industry, wholesaler MCB and Tata Steel have gone live with Smart Connected Supplier Network (SCSN) for a number of materials. This means that the ERP system automatically places Tata Steel's orders for those materials directly in the wholesaler's ordering system. In turn, MCB exchanges data with TataSteel via the SCSN network. Both parties are able to continue using their own ERP system and internet platform because the SCSN standard ensures interoperability between the systems.

Impact on the data landscape and cloud architectures in the EU

We expect that the topic of data sovereignty will become an ever-more important factor for organisations when defining their data strategy – alongside the existing considerations of flexibility, innovation, costs, connectivity and IT management.

Although the EU-funded initiatives aimed at advancing data sovereignty are largely conceptual, they will help to overcome the data sovereignty challenges that businesses are facing, for instance when working with cloud architectures needed to deploy new or upgrade existing process/manufacturing software. We are encouraged by the positive results that are already emerging and believe that many more initiatives will soon follow, providing the focus continues to be on adoption and commercialisation of the available technology.

Author

Mariane ter Veen and Douwe Lycklama

ORIGINAL BLOG

GET IN TOUCH

BLOG

Three essentials for unleashing the full benefits of data

1 July 2020

Mariane ter Veen

Guest author:
Jyrki Suokas

The European Commission wants to make Europe fit for the digital age and unleash the full benefits of better data usage. In order to achieve this ambition, we believe that it is first necessary to make data sovereignty a design principle, develop a soft infrastructure and focus on adoption.

The new data strategy published by the European Commission aims to make the EU a leader in a data-driven society. It seeks to create a single market for data that will allow it to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations.

At Sitra and INNOPAY, we fully support this ambition. However, we believe that it can only be successfully achieved if the following three essentials form the basis for implementing the data strategy:

1. Data sovereignty as a design principle

Data sovereignty – self-determination over data by both individuals and companies – should be an underlying key design principle for the execution of the European Data Strategy. Individuals or organisations are self-determining when they have the capacity to control who has access to their data and under what conditions. We don't discriminate here between personal and non-personal data. After all, organisations' data-driven services are ultimately mostly consumed by individuals and the usage of personal data improves the quality of those services.
A focus on data sovereignty reflects our European values and sets Europe's data model apart from today's other two dominant models (the 'winner takes all' platform model

based on individuals as market actors, and the state-led data-sharing model). In fact, data sovereignty is already embodied in European legislation; the GDPR has given citizens the 'right' to data sovereignty, but not yet the means to execute that right – so there is still work to be done.

But this is both feasible and worthwhile, because data sovereignty offers benefits for all roles in the data-sharing ecosystem. It allows citizens and organisations to permit sources holding data on their behalf (e.g. telecom companies, utilities, banks, trading partners, etc.) to use that data for specific purposes and/or to share it with other authorised parties. It also enables citizens and organisations to withdraw their consent at any time.

2. Soft infrastructure because it's all about access

Data is essential for the creation of new business models for data-driven innovations and services. However, a growing unwillingness to share data due to privacy and security concerns on the one hand, and the inability to share data due to a lack of interoperability on the other, are standing in the way of access to sufficient data.

An enterprise architecture view of data governance is needed to ensure data sharing within sectors and across sectors. At the moment, the discussion around data governance happens mostly inside sectors and in individual projects and tends to emphasise just one or two different aspects, such as technology, legislation or business models. It is difficult to create a common governance framework when there is a lack of common concepts and semantics. In order to bridge the gap, the European Commission should look into establishing an EU trust framework for cross-sectoral data governance. This should be built around easy-to-grasp and actionable guidelines encompassing all relevant aspects: business, legal, ethical and technical.

This 'soft' infrastructure or afsprakenstelsel will serve as the basis for managed data sharing in the future, just as hard infrastructure (such as waterways, roads, railways, sewers and the electrical grid) has been the foundation of health, wealth and economic growth through the centuries. An afsprakenstelsel could facilitate how to deal with consent. We believe that the European Commission should try to avoid regulating per sector ('point regulation' or regulation per use case) wherever possible and focus on principle-based regulation instead. After all, the adoption of telecoms, payments and internet is not defined per sector either.

In our view, the quickest and most effective regulatory intervention would be to make data sovereignty mandatory for businesses and the public sector in the coming decade for both personal data and business data alike. That can be done in just a few steps, if the 'how' (interoperability, trust, standards, governance, level playing field, certification, adherence, etc.) is clearly distinguished from the 'what' (sector use cases/applications). In that case, only the application is sector-specific and will require additional implementation guidelines and associated governance.

3. Focus on adoption, not on technology

A crucial yet often undervalued aspect of new advancements is communication and awareness building towards end users. This is especially true for the European data sovereignty infrastructure, as this is a new concept which will manifest itself in all 'B2G2C' services such as business-to-consumer (B2C), business-to-business (B2B), business-to-government (B2G), government-to-business (G2B) and government-to-consumer (G2C) services. We believe that, with the right focus on adoption, it is possible to educate the European population and subsequently the global population on the benefits of a new, empowered approach to data, just as happened in the past in the case of mobile telephony, payments and messaging, for example.

Easy-to-grasp paradigm based on European values

Based on European values and the concept of data sovereignty, the European Data Strategy provides the necessary direction to unleash the full benefits of better data usage in the EU and create a thriving human-centric data economy.

We believe that the shortest and most effective intervention in order to ensure this succeeds in practice is to make data sovereignty mandatory over the coming decade. It's an easy-to-grasp paradigm that can be introduced in just a few steps – supporting short-term implementation and adoption, yet also allowing the time needed to develop the accompanying fit-for-purpose regulatory framework.

The aim should be to nudge businesses and governments (and their IT providers) into giving their users, customers and citizens tools to manage, share and exploit their data. This should include ways to monetise/compensate for data benefits. Ultimately, this will accelerate the execution of the European Data Strategy and ensure that the EU becomes a leading role model as a society empowered by data.

Authors

Mariane ter Veen and Jyrki Suokas

ORIGINAL BLOG

GET IN TOUCH

BLOG

EPI: Paving the way for future bank relevance, and not just through payments

8 July 2020

Mounaim Cortet

Sixteen major Eurozone banks have come together in the European Payments Initiative (EPI) to launch a new payment system aimed at taking on rival card schemes and the threat posed by Chinese and US big-tech firms. Although previous pan-European collaboration projects (e.g. Monnet, Eaps, Payfair) have not been perceived as a great success, the mounting competitive pressure and challenging market dynamics are now driving banks back together.

EPI is seeking to develop a unified payment solution for consumers and merchants across Europe, including a payment card and digital wallet, covering in-store, online and person-to-person payments as well as cash withdrawals. INNOPAY shares the view that EPI is a worthy step towards strengthening Europe's payments landscape, providing that it leverages existing best practices where possible and receives the full and continued support of all relevant banks.

However, the initiative seems to have emerged as a result of political pressure from the European Central Bank's call for more collaboration, rather than out of a desire to pursue true customer value. That is, compared to the solutions available today, it is not likely to fundamentally improve the way people actually pay at the point of interaction, nor will the initiative in its current form be an answer to banks' quest for future relevance.

In essence, the EPI collaboration is a good start, but the battlefield for banks' future relevance is much broader than payments alone. If anything, the banks involved should leverage this collaboration platform and momentum to shape their future relevance. That is why we urge the banks involved in EPI to take a broader view of digital transactions. In other words, in addition to payments, banks need to actively address the topic of digital identity and seamless data sharing. This will not only drive the creation of truly value-added services, but will also strengthen their competitive position. While we understand the EPI's current scope and focus on protecting the business case for payments (which is also supported by the European Commission's decision not to impose further legislative measures on interchange fees for now), the new battle revolves around identity and data – and even more value is at stake.

Need for new type of trust infrastructure in Europe

For banks to reap the full benefits of the data economy, Europe needs a new type of trust infrastructure based on digital trust. This will allow us to move away from the closed, institutional trust-driven approach that is 'forced' upon users by the big-tech firms. The key components of such an infrastructure are depicted in Figure 1.

In the digital trust infrastructure, common standards for data rights and obligations are embedded in the very fabric of the internet ('transactional internet'). A federated and trusted digital identity is fundamental in such an infrastructure. Connected to this digital identity is a consent and authorisation mechanism that enables end users to control their money and data. An electronic interoperable payments network and data exchange layer can then be built on top of consent. This approach enables data availability and accessibility at scale to power new applications in payments and the broader data economy. Ultimately, this leads to better protection of user data and privacy, greater innovation at scale and creation of new business models and value exchange, thus safeguarding banks' future relevance.

Banks are well placed to create the digital trust infrastructure

"What makes banks so well placed to create the digital trust infrastructure?" I hear you ask. This is due to three key reasons: positioning, experience and assets.

Firstly, banks have always been positioned as a 'money custodian'. Becoming a 'data custodian' (in a much broader sense than they already are) in the digital economy would be a natural extension of this role. More importantly, while players from other industries are still winning trust – especially among the younger generation – banks have a head start that they should be able to leverage. The broader public are more likely to accept banks than other players in this role.

The second factor is experience. As data is becoming increasingly valuable in the digital economy, there is a strong rationale to apply 'digital payment-like' governance and mechanisms to ensure trust in the envisioned digital trust infrastructure. Banks have the necessary experience with schemes to turn the digital trust infrastructure into reality.

Thirdly, banks have the required assets. Besides having an exemplary role, banks are also very proficient at determining consumers' digital identities due to their Know Your Customer (KYC) obligations. Thanks to these digital identities and strong customer authentication (SCA) mechanisms, banks can already play a key role in giving consumers control of personal data in other sectors. After all, consumers must be identified with

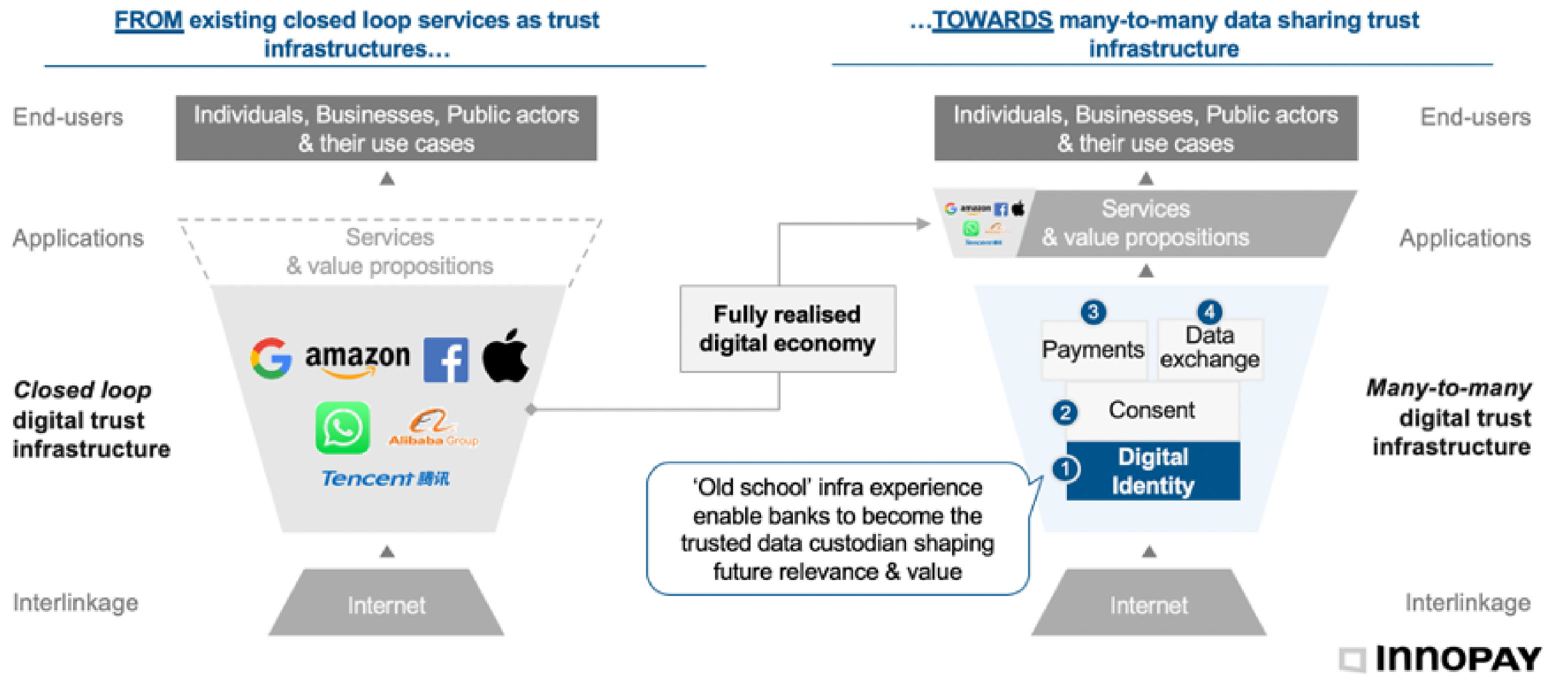

FROM existing closed loop services as trust infrastructures…
…TOWARDS many-to-many data sharing trust infrastructure
End-users
Individuals, Businesses, Public actors & their use cases
Applications
Services & value propositions
Closed loop digital trust infrastructure
amazon
Tencent 腾讯
Alibaba Group
Fully realised digital economy
3 Payments
4 Data exchange
2 Consent
1 Digital Identity
Many-to-many digital trust infrastructure
'Old school' infra experience enable banks to become the trusted data custodian shaping future relevance & value
Interlinkage
Internet
INNOPAY

Figure 1: Four key components of the digital trust infrastructure, INNOPAY 2020

sufficient reliability if they are to irrefutably authorise other parties to use particular data (which is why digital identity is positioned as the core building block in Figure 1). Furthermore, the mandatory opening up of banks under PSD2 has enabled them to gain experience in obtaining and managing authorisations from consumers. Each authorisation must be recorded securely and reliably so that the consumer always has an up-to-date overview of the parties which have been given access and, if desired, can also withdraw their consent for that access. This experience, combined with digital identity, is an important asset that can be deployed beyond the confines of payments and banking. By turning this experience into services, banks can take a significant step towards facilitating the data economy in other sectors.

Over to you

We all know that developing a scheme for a digital trust infrastructure requires collaboration – initially with banks in the pioneering role as outlined above, followed by the subsequent involvement of other private-sector operators. In addition to shaping the collaborative domain of the digital trust infrastructure, banks will also need to develop a clear view of their individual competitive position, strategy and value proposition within such a network.

The banks involved in EPI have already cleared the first hurdle by agreeing to collaborate on payments. They now need to shift up a gear to truly strengthen European banks' position in payments and the data economy by developing innovative services that add true customer value. It is time for banks to work together to create a digital trust infrastructure and reinforce their position as trusted data custodians.

Author

Mounaim Cortet

ORIGINAL BLOG

GET IN TOUCH

BLOG

INNOPAY Open Banking Monitor: Increasing API focus on business and community context

27 July 2020

Mounaim Cortet

Jorgos Tsovilis

Marloes Blankert

Banks need to get their Open Banking strategy right. Our research indicates that banks seeking to claim a solid position in the Open Banking landscape will need to move beyond merely offering high-quality documentation, sandboxes, developer tools and seamless access to APIs. That is, banks need to build, grow and nurture their Open Banking community to strengthen their position and accelerate their commercial efforts. In our view, banks that get their Open Banking strategy right will establish credibility and a footprint in the data economy as a stepping stone for future relevance and new business models.

Over the past months we've seen banks continuing to build upon their Open Banking offering, publishing rich API catalogues or focusing on providing a solid Developer Experience. In addition, various newcomers have positioned themselves in the Open Banking landscape and made their debut in our Open Banking Monitor (OBM): HSBC (Hong Kong), ICICI Bank (India), KBC (Belgium), Nedbank (South Africa), Raiffeisen Bank (Australia), Spar Nord (Denmark), US Bank and Wells Fargo (United States).
In this latest release of the OBM, updated in May 2020 (see Figure 1), we take a look at the new status quo, highlight a number of best-in -class examples and identify two trends that Open Banking business owners need to consider in order to accelerate.

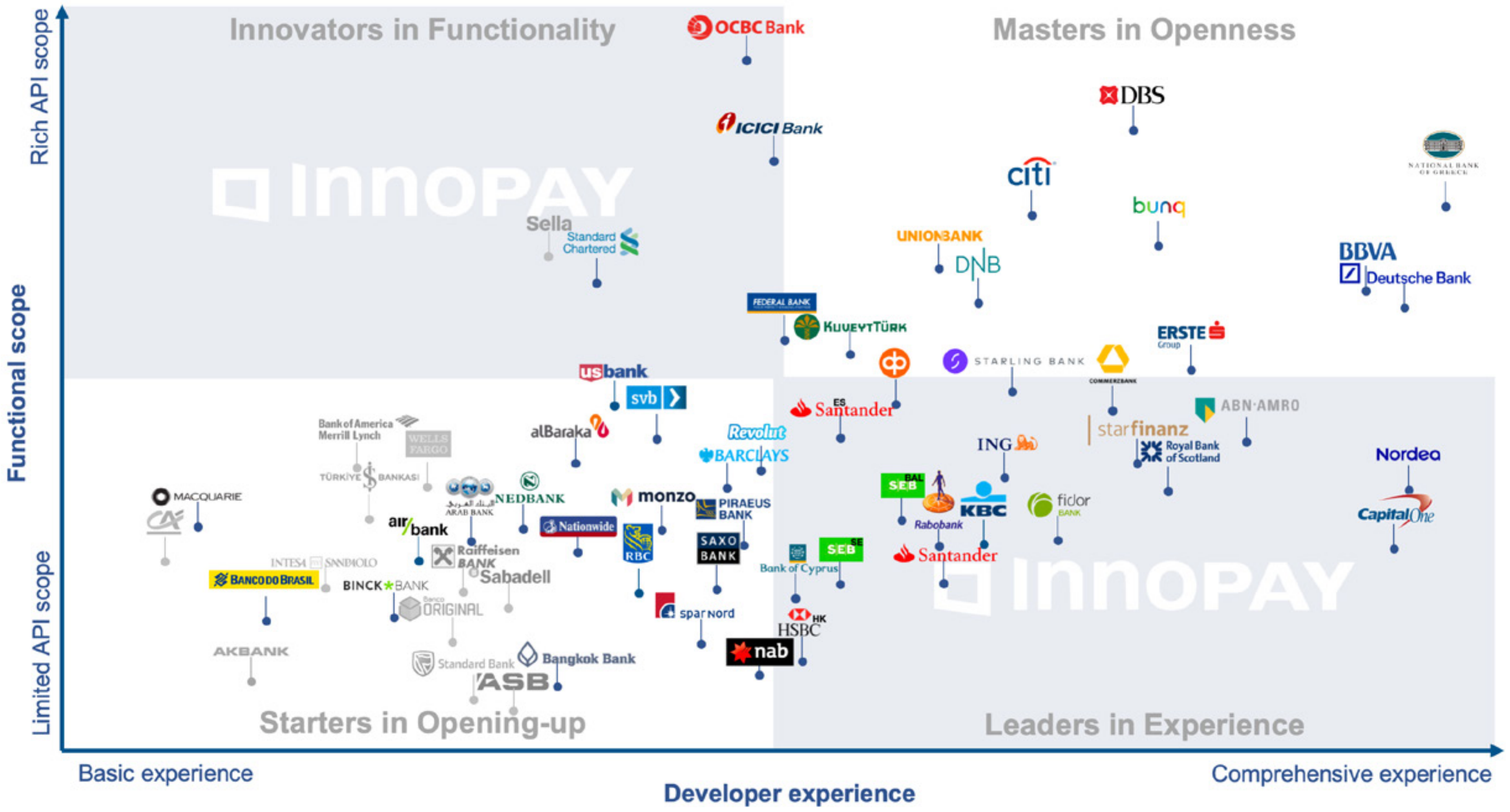


Figure 1: The INNOPAY Open Banking Monitor (updated May 2020)

Highlights from selected best in class banks

Since our previous update of the INNOPAY OBM (August 2019), many banks have continued to build upon their Open Banking offerings, with new APIs and features contributing to a better Developer Experience. Analysis using our Capability Model reveals different best-in-class banks in each category rather than a single clear winner (see Figure 2).

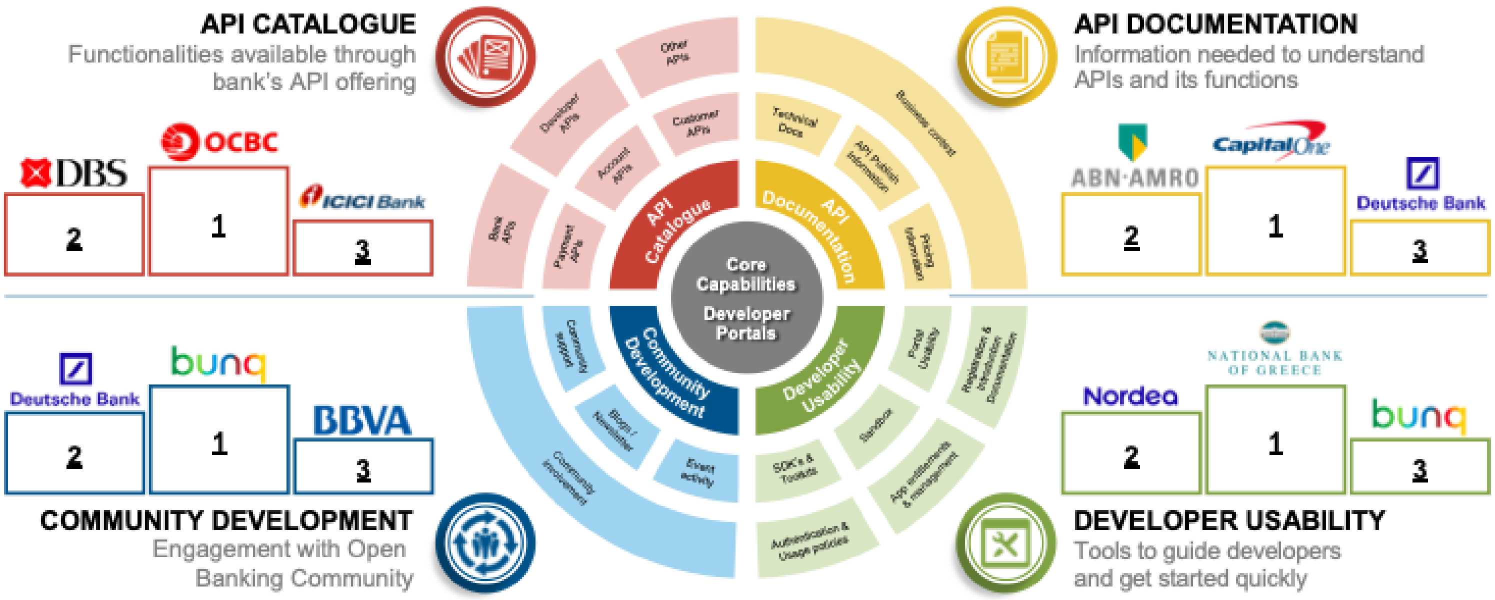


Figure 2: Best in class banks in the OBM (updated May 2020)

To elaborate on some key developments, we first highlight newcomer ICICI Bank. Firstly, with at least 250 APIs, ICICI Bank has quickly positioned itself as an 'Innovator in Functionality' and even become a top-3 performer based on its impressive API Catalogue. For customer identification and authorisation, ICICI Bank leverages India's Aadhaar infrastructure. Combined with India's sector-wide API strategy as part of the India stack, this indicates that we can potentially expect more Indian banks to start releasing their Open Banking services soon. Secondly, the National Bank of Greece has made a significant leap forward and now offers the best combination of a rich API Catalogue and Developer Usability. The National Bank of Greece offers a wide variety of developer tools, ranging from SDKs to Swagger and Postman files. Additionally, it offers a virtual programming environment for developers to manage and develop their projects.

Lastly, we want to highlight Bunq's impressive updates that have propelled it from being an 'Innovator in Functionality' to a 'Master in Openness'. One particularly interesting development is the combination of two functionalities; Bunq's 'Access to Own Account' allows its users to access their own account details through APIs and then share the resulting applications through a dedicated GitHub repository. This enables the whole community to contribute by continuing the development of these applications and adding new features. Overall, a wide variety of GitHub repositories and community projects are available, allowing practically anyone to create an Open Banking application connected to their own account. This is perhaps an interesting glimpse of the potential of Open Banking and how it might evolve. As the best-in-class example in the Community Development category, Bunq provides real-life examples of how to involve the community and increase engagement amongst users and developers.

Banks' increasing focus on creating a business-minded open banking community

Now that our Open Banking Monitor has tracked the Open Banking landscape for some years, certain changes and trends are becoming more evident. As depicted in Figure 3, two key trends are:

1. Bank API portals increasingly focus on business-minded visitors
2. Community development efforts rise slowly but steadily

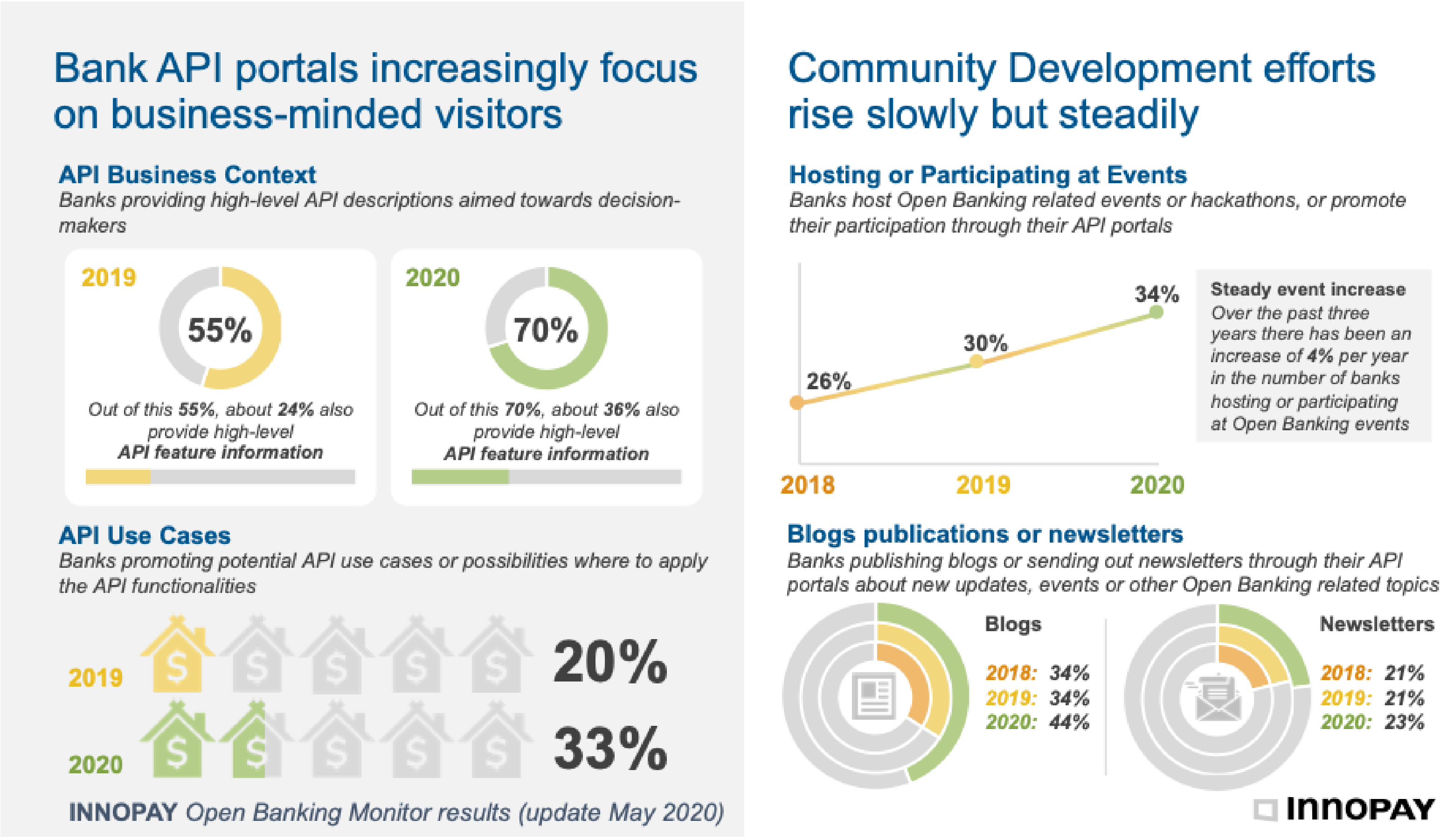


Figure 3

1. Bank API portals increasingly focus on business-minded visitors

To ensure that the more business-minded visitors are triggered too, banks increasingly cater for a wider audience on their API portals. As identified in our previous OBM release (August 2019), business focus can be increased by providing high-level descriptions, API features and information on potential use cases. Partner use cases and testimonials promote creditability of brands and products, and substantiate customer satisfaction. When comparing the number of banks with API Business Context information in 2020 against 2019, a significant increase can be observed. Approximately 70% of the developer portals included in the OBM now provide some form of high-level API descriptions. Of them, about 36% go the extra mile by offering additional business context through API feature information (i.e. a clear overview of the data available through the API). In addition, the number of banks providing information on potential API use cases or successful case studies has risen from one in five to one in three. To some extent, the growing use of case studies is likely to be related to the fact that many banks are gradually building up their portfolio of partnerships and success stories as Open Banking gains more traction. By choosing to publish this information on their API portals, however, the banks demonstrate greater awareness of their target groups; developers are no longer the only ones looking to consume APIs, but developer portals are now also used by less technically skilled and more business-oriented visitors.

2. Community development efforts rise slowly but steadily

As shown in Figure 3, over the last three years the number of banks that host or participate in Open Banking-related events has increased by 4% annually. This does not necessarily imply that banks are hosting or attending more events. Instead, it indicates that they are more open and communicative about these efforts through their API portals in general. In addition, over the past year there has been a rise in the number of banks with a blog or article section on their developer portal, where they publish news items about updates, recaps or teasers about events or other Open Banking-related topics. All of these developments are centred around an increase in communication towards the existing and potential visitors to the API portal. This increase can be seen as evidence of these banks' stronger marketing efforts to develop a broader Open Banking community, thereby increasing brand recognition as an authority on Open Banking and promoting engagement and product development idea generation. Different Open Banking communities serve different purposes depending on each bank's chosen Open Banking strategy. Combined with the increasing number of possibilities that are enabled through Open Banking, such as new APIs, we are starting to see just how much potential such communities can have. Whether through collaboration on open-source projects or by hosting hackathons with fintech partners, the importance of a solid community has attracted considerable attention over the years.

True potential of open banking communities

Overall, it comes as no surprise that many of today's frontrunning banks are now reaping the benefits of their solid communities to keep them ahead of the pack. The true potential of an Open Banking community starts to become apparent when the two trends stated above (i.e. focus on a broader business-minded public and increased community development efforts) are combined. In order to give the subject of community development the attention it deserves, our article on 'Building and leveraging an Open Banking community' dives deeper into three key considerations for banks when developing a community. It also discusses a variety of approaches for banks looking to further enhance their Open Banking communities as a cornerstone of future relevance and new business models.

Do you wish to learn more about 'Building and leveraging an Open Banking community'?
Download our article

INNOPAY's experience and services portfolio can help banks and non-banks to design, launch and scale their Open Banking strategy. We have recently initiated a campaign to share our strategic perspectives on the role of Open Banking in establishing a strong footprint and credibility in the data economy.

If you want to know more, reach out to discuss these perspectives and the opportunities for your organisation. Stay tuned for more updates from the INNOPAY Open Banking Monitor.

Authors

Mounaim Cortet, Jorgos Tsovilis and Marloes Blankert

ORIGINAL BLOG

GET IN TOUCH

BLOG

Why banks must become the data custodian in the data economy

30 July 2020

Mounaim Cortet

The rising importance of digital identity, consent management and data sharing has created a 'Blue Ocean' market for banks. I believe that they now have a unique opportunity to strengthen and truly safeguard their relevance in the data economy. But they need to start taking decisive action right now in order to demonstrate that they can provide the necessary trust.

The European Payments Initiative (EPI) is an important collaboration platform and a clear step in the right direction. However, the banks involved in the EPI currently appear to be focused on protecting the payments business case in Europe. While this is understandable, such defensive tactics in the 'Red Ocean' payments market is not really a viable long-term strategy. The good news is that, as we see it, the EPI also paves the way for strengthening the banks' future relevance – beyond payments alone.

The opportunity for banks to secure their future relevance

Regulatory reforms such as PSD2, Open Banking, GDPR and developments such as the EU Data Strategy are democratising access to data assets across the whole economy. In this changing world, banks now facilitate only a fraction of a customer's (daily) digital interactions and transactions. However, as money custodian, banks are ideally placed to expand their role into the data domain. In other words, we believe that banks can – and should – lay claim to the role of 'data custodian' in their customers' daily lives by engaging in a cross-sectoral data ecosystem (see Figure 1) – just as they do in their current role in payments.

Ultimately, the role of data custodian will help to secure the future relevance of banks in the data economy in several ways, including by:

- Offering better protection of user data and privacy
- Driving innovation in digital transaction services (payments and beyond)
- Stimulating the creation of new business models and monetisation options
- Effectively shielding them against threats coming from Chinese and US big-tech firms.

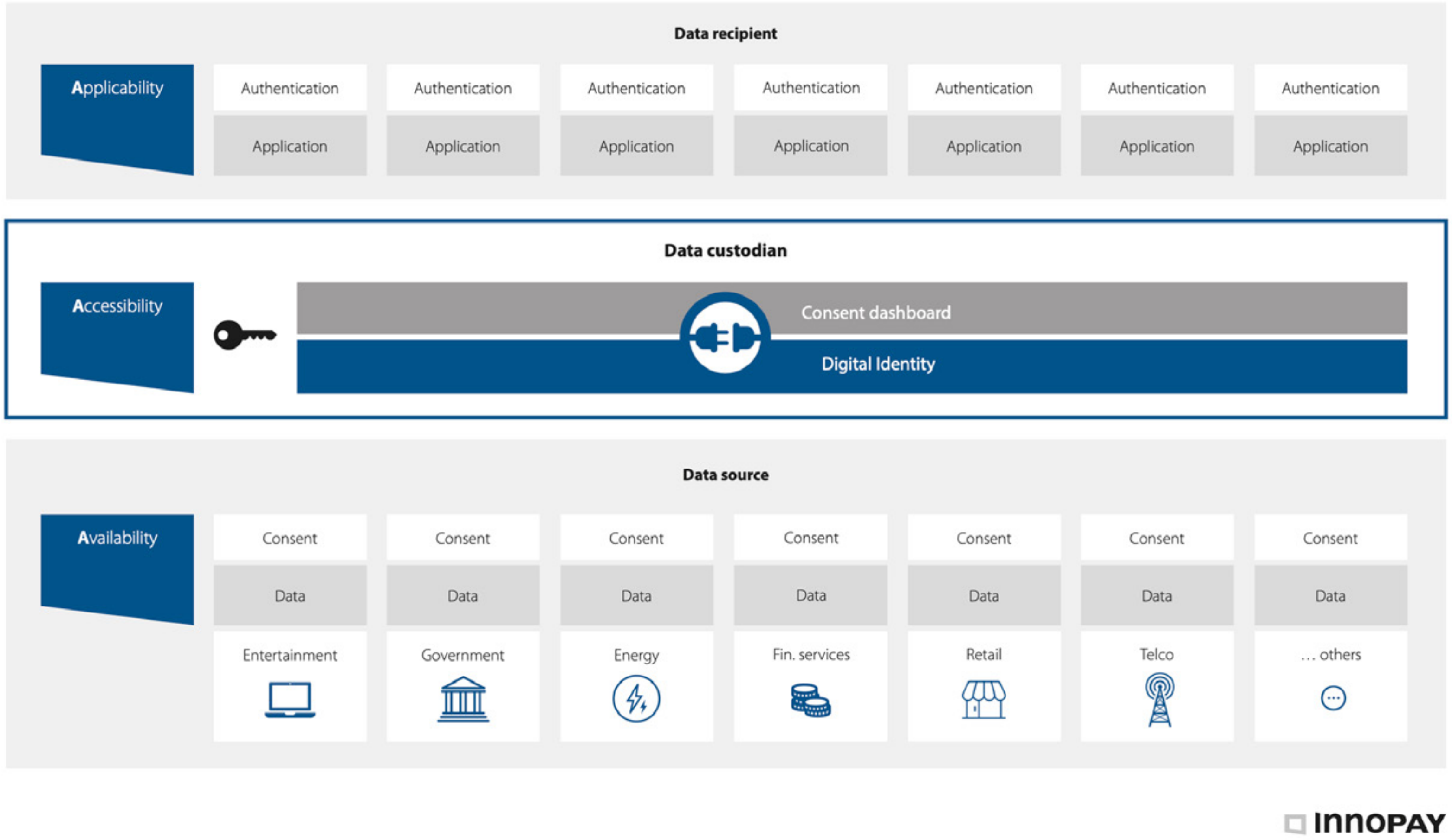


Figure 1: Banks acting as data custodian in the data economy

The shifting data-benefit balance

In a changing world in which data is emerging as the new global currency and digital transactions are at the heart of everything we do, customers are becoming more aware of their data assets and the value it represents; they want to leverage their data beyond the platforms and organisations that store it in order to tip the 'data-benefit balance' back in their favour. This is driving customer demand for increased transparency and control over their data assets – which is also known as 'data sovereignty'.

As a result, we are seeing an emerging need for a data custodian like role to ensure seamless and secure access in a trusted and well-governed ecosystem which revolves around digital identity and consent. Trust provision will be a key functional domain. The data custodian will meet the growing desire among customers to have a single point of control for their data assets, including by giving customers the required tools to exercise control over them. In addition, as customers become accustomed to controlling and sharing their data on their own terms, the increased trust will open up new opportunities to engage in ways that create customer-centric data monetisation models and a fair distribution of the benefits.

The three key beliefs shaping the future relevance of banks

Against the backdrop of the current transformation, we believe that the future relevance of banks will be shaped by the following three beliefs:

1. Although important, digital payments – and related collaborations (e.g. EPI) – are not sufficient for banks to

remain relevant in a world in which everything is a digital transaction

2. Banks are ideally placed to unlock the potential of the open data economy by creating a digital trust infrastructure and become society's everyday data custodian
3. In an open data economy, a bank's digital identity and consent management services are key in facilitating trusted financial and non-financial digital transactions in all areas of society.

So bank executives face a choice. They can either ignore the digital transaction revolution and stick to their existing beliefs, continuing to invest in payments only and competing head-on with big-tech and other players in a Red Ocean market… or they can embrace the above beliefs to seize the Blue Ocean opportunity, expanding their role as money custodian into the data domain to secure their future relevance in the data economy.

Becoming a data custodian in the data economy is a longer-term play; it requires bank executives to embark on strategic initiatives that do not necessarily contribute directly to short-term regulatory compliance and/or ROI. However, doing nothing is not an option as the true battle for relevance revolves around digital identity, consent and data sharing – where even more value is at stake than in payments. As big-tech firms and other providers are already making inroads into these areas, there is no time to waste.

Leaders at any bank wishing to participate successfully in this new environment will need to review their strategies as well as their technological and operational capabilities. Banks will have to recognise that putting customers in control of their money and data is imperative for future strategic and commercial relevance.

Author

Mounaim Cortet

ORIGINAL BLOG

GET IN TOUCH

BLOG

How much Open Banking budget is future relevance worth to you?

2 September 2020

Shikko Nijland

It is time for banks to reconsider their perspective on Open Banking. In this new transaction- and data-driven world, data sharing – just like money and payments – needs to be decentralised. However, it must also be interoperable and trustable. Proper governance and oversight safeguard public functions for society as a whole, and data sharing should be no exception. INNOPAY believes that banks are currently in a unique position to outperform Big Tech challengers by leveraging their core capabilities, infrastructures, operating models and experience in payments and transactions, with a special focus on digital identity. But that requires investment in Open Banking now – before it's too late.

In spite of regulations like PSD2 and GDPR, the volume, value and complexity of data is still growing much faster than we can cope with as a society. This poses particular challenges when it comes to data sharing and related issues regarding privacy, data sovereignty and the data benefit balance. Our societal inability to understand, regulate and control the new rules of the game has resulted in a shake-up of virtually all market and economic positions. We find ourselves in a new data-driven world in which the winner takes it all. A handful of large players are now dominating entire sectors, and this is creating relentless network effects in terms of customer reach and data richness. Data has become geopolitics and people no longer feel that they live in a digital data democracy that mirrors and embraces the same principles as their real-life democracy.

Apart from introducing draconic legal or regulatory measures aimed at putting people back in control of their data, the most feasible and effective option is to disrupt the underlying root causes of the exponential data network effects. This can be achieved by creating a decentralised yet interoperable approach to data sharing based on a foundation of undisputed trust. This requires not only cross-border reach, but also a wide range of technology, appropriate global and local legal frameworks and reliable operations – and banks already have precisely all these capabilities. Moreover, banks have learned about the importance of interoperability the hard way and they have extensive experience of setting up and running similar schemes and trust frameworks related to payments. In our view, doing the same for data sharing is a logical next step.

From money to data custodian

There is a fast-diminishing window of opportunity for banks to evolve from being a 'money custodian' into a 'data custodian'. In fact, this evolution holds the key to safeguarding their future relevance and value. Besides payments, banks have the opportunity to take a leading role as a facilitator, enabling citizens and companies to exchange data securely and fairly. For example, identity can be regarded as the essence of data sovereignty; it provides the crucial legal link to data entitlement by individuals and businesses. In this context, banks can reinforce their role as a trust provider by offering digital identity propositions. Additionally, instead of merely being compliant with GDPR and PSD2, banks can provide their customers with concrete means and tools to actually control their own data. Open Banking should be repositioned as 're-use your data safely elsewhere'.

In order for the banking sector to carve out this new position and establish a sustainable, sizeable and profitable footprint in the data economy, banks need to increase their Open Banking budgets rather than rationalising them. Within most organisations, the budget discussions usually begin after the summer holidays. Therefore, if banks have the ambition to become a trusted cornerstone of society once more, now is the time to secure sufficient funding to invest in Open Banking data and API capabilities. By thinking ahead, banks can address not only current, but also upcoming data legislation. By working together as a sector, they can pool their defensive strength to lock out GAFA and establish more balanced and sustainable trust partnerships in any community of interest.

Ultimately, the size and depth of your Open Banking footprint will determine how fast you can evolve from a money custodian into a data custodian and secure your future relevance and value by developing new business models. How much budget is that worth to you?

Author
Shikko Nijland

ORIGINAL BLOG

GET IN TOUCH

BLOG

The American Central Bank Digital Currency plan – quiet, powerful, imminent

7 September 2020

Douwe Lycklama

Douwe Lycklama, INNOPAY: After years of cash reduction in favour of commercial banks debt money, now central banks can regain some of their position once held in a cash society

This article is originally published on the Paypers.

There hasn't been too much media around Central Bank Digital Currency (CBDC) plans/ projects coming from the US. So far Libra, China's digital yuan initiative, also known as DCEP, and Sweden's digitalisation plan have captured the public attention. However, the US has taken strong steps towards adopting digital currencies and in the coming months, we can expect a further acceleration of these.
We continue our series on the topic of Central Bank Digital Currencies and today we are speaking with Douwe Lycklama, co-founder of INNOPAY and co-author of 'Everything Transaction' to learn more about US' plan to drive CBDC adoption.

Substantial development is the somewhat unnoticed bill 'Banking Act for All', where potentially all US citizens may end up with a 'digital dollar wallet' at the FED. The bill was put to congress already on March 23, 2020 and discussed on a public hearing on June 30, 2020. The project group has published a white paper in May 2020.

The bill outlines that (starting with January 1, 2021) banks must offer these wallets legally segregated from their operations, with the similar functionalities (apps, cards, web) as regular payment account and a no additional cost to customers. The balance of the wallet corresponds one-to-one to the balance of central bank moneys (M0) held by the bank offering the wallet. Adoption is ensured because 'COVID relief funds' will be distributed through this FED digital dollar system.

Why is this big? For the first, time citizens get a digital version central bank money, a.k.a. digital cash, or Central Bank Digital Currency (CBDC). That is FED money, which is full reserve, primarily not made of debt created in the commercial banking system. Today only banks and some market infrastructures can hold an account at the FED.

If all this happens, the CBDC isn't a theoretical topic anymore. Some considerations:

1 Citizens may find it more attractive to hold their balances in their FED wallet and move their money away from commercial banks. This puts pressure on commercial banks, as this is the digital version of the much-feared 'bank run', something to consider carefully when implementing. After years of cash reduction in favour of commercial banks debt money, now central banks can play their part more. At the same time banks will remain crucial for mass customer contacts such as KYC, AML and the overall account and payment proposition. A different business model may be required for CBCDs flowing through the existing 'plumbing'.

2 CBDC enables governments to directly stimulate the economy down to every citizen through 'helicopter money', a term coined by Ben Bernanke already in 2002, as a policy option to counter deflation. Today's fiscal stimulus through 'quantitative easing' programs mainly inflates financial assets and therefore has difficulty reaching the population at large. On August 27, 2020 FED's president Jay Powel announced a more aggressive continuation of the US inflationary policy [link]. CBDC's direct reach may help toward this goal.

3 Libra's initiative will provide a global infrastructure for digital token exchange, complementing and accelerating the already existing nascent infrastructures of Bitcoin and Ethereum. CBDC can use this new infrastructure as well, by integrating the FED digital dollar system into these rails. This increases the utility of CBDC as it will have a global reach instantly. This also helps to enforce the US dollar position in the world economy. A second order effect of the adoption of different rails may be the acceleration of Decentralised Finance (DeFi), a movement aimed at replicating some core function of the financial systems, such as checking account, lending, saving and asset trading.

4 CDBC potentially can be made 'programmable' by giving them specific functionalities, e.g., some tokens can be interest bearing, some tokens can only have a designated spending goal or tokens can trigger tax collection. The latter will reduce today's cash-driven informal economy, while the other functionalities influence its application.

The FED is not alone with its CBDC project. Other jurisdictions are working on this as well, notably the Eurozone, Japan, Sweden, UK, and, last but not least, China with their digital Yuan, coinciding with their global BSN blockchain initiative. On August 29, 2020 the Chinese had a supposedly secret soft launch but was pulled back fast when more people than expected showed interest.

In the coming months a lot of developments will come together and propel CBDC into reality: the economic downturn triggered by COVID, fiscal stimulus by governments worldwide, Libra's introduction, crypto-technologies maturing, citizens seeking refuge for their savings, financial inclusion drive and of course the on-going geo-political currency wars.

Author

Douwe Lycklama

ORIGINAL BLOG

GET IN TOUCH

BLOG

Six criteria for selecting an API connectivity provider to power your PSD2 opportunities

2 October 2020

Luc van Oorschot

Annabel Keulen

When you are working on PSD2 opportunities, it is of the utmost importance to select the right API connectivity provider. Their technology capabilities can greatly assist you in launching a successful PSD2 proposition for your customers, while accelerating your development process and time to market. This blog helps you to apply the right criteria to inform this important strategic decision.

Once you have decided to outsource the API connectivity work (see our previous blog for insights in what considerations influence 'make or buy' decisions for API connectivity providers), you will discover that there are many different API connectivity providers, both with and without a PSD2 licence. That's why it is so important to select the right API connectivity provider who will power your PSD2 opportunity. Note that there is no one-size-fits-all approach; the relevance and relative weighting of the selection criteria listed below must take the specific context and business requirements of the respective PSD2 opportunity into account. Additionally, bear in mind that service providers need to grow with your organisation as the PSD2 proposition matures and criteria evolve.

The six selection criteria

1. Connectivity reach

The reach of providers – that is, the number of connected banks per country – differs greatly, with many local and regional providers operating in the market. It is important that an API connectivity provider covers the geographical scope required for your PSD2 opportunity, as this ensures that you are not required to contract and integrate with multiple providers to establish the required reach among banks that you want to include in your service. API connectivity providers often prioritise their connectivity roadmap based on client demands. This is an important aspect to realise when you have strict timelines for realisation of your PSD2 opportunity.

2. Functional scope

There can be differences between the functional scope of different API connectivity providers' service offerings, as they often focus on additional white-label services on top of the core connectivity to bank APIs. Three types of white-label service offerings are typically distinguished:

1 'Raw' API connectivity: technical aggregation of available bank APIs for PSD2 account information and payment initiation. This is typically extended with other 'premium' bank APIs and/or APIs providing access to other organisations and respective data sources/capabilities. This functional offering forms a ticket to play for service providers and is more a qualifier than a differentiator.

2 Feature-rich functional components: functionality that is added to the raw API functionality, such as specific processing of data or detailed analysis of payments data to identify patterns as a basis for value-added advisory services. Examples of service providers in this category include, among others, Invers, Fintecsystems, Plaid and Budget Insight.

3 White-label applications: fully fledged products and capabilities that are offered as a service for branding by client-facing organisations (B2C or B2B). Examples of service providers in this category include, among others, Minna Technologies, Tink, Moneyhub Enterprise and Yolt Technology Services.

Figure 1 provides a high-level overview of the different services per category that are offered by API connectivity providers.

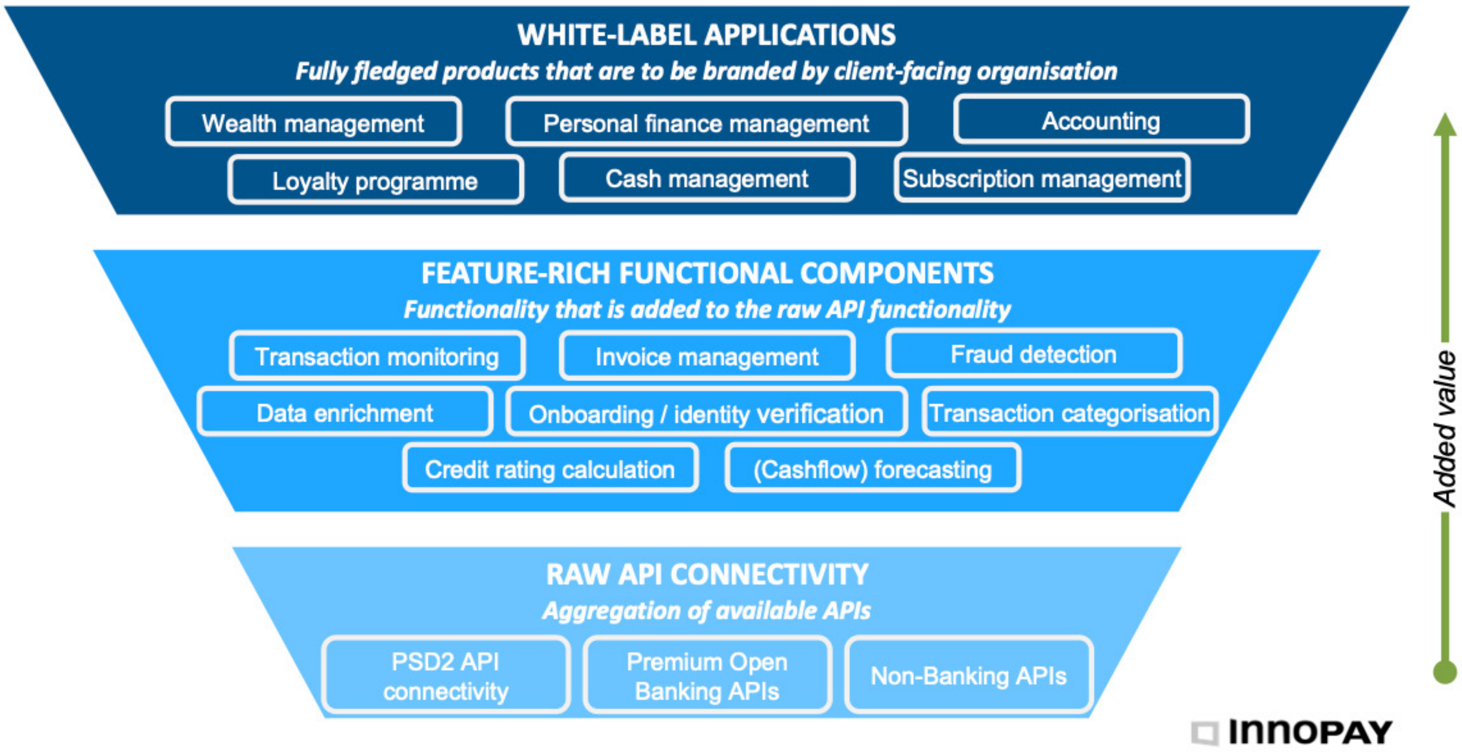

WHITE-LABEL APPLICATIONS
Fully fledged products that are to be branded by client-facing organisation
Wealth management
Personal finance management
Accounting
Loyalty programme
Cash management
Subscription management
FEATURE-RICH FUNCTIONAL COMPONENTS
Functionality that is added to the raw API functionality
Transaction monitoring
Invoice management
Fraud detection
Data enrichment
Onboarding / identity verification
Transaction categorisation
Credit rating calculation
(Cashflow) forecasting
RAW API CONNECTIVITY
Aggregation of available APIs
PSD2 API connectivity
Premium Open Banking APIs
Non-Banking APIs
Added value
INNOPAY

Figure 1: Overview of different types of services offered by API connectivity providers.

3. Licence-as-a-Service

As detailed in our previous blog, some situations do not require you to have your own licence to enable your PSD2 opportunity, in which case you can save costs and resources that would otherwise be involved in obtaining and maintaining a licence. If this applies to your situation, the API connectivity provider must have a PSD2 licence in order to support you. There are currently 89 parties operational in Europe that have a PSD2 licence and offer API connectivity services.

4. Connectivity to other data sources

PSD2 is a legal mandate for banks to open up specific data and functionalities for payment account information and payment initiation. There are, however, other valuable data sources available that could be relevant for your PSD2 opportunity, e.g. premium bank APIs that open up functionalities and data outside the scope of PSD2 and non-bank data sources from organisations operating in other sectors. Examples of such non-bank data sources are Chamber of Commerce, National Vehicle Authority and geodata. Some API connectivity providers offer connectivity to (a selection of) these additional data sources through various technologies (e.g. APIs, screen scraping, reverse engineering).

5. Cost

The pricing models used by providers vary widely. Some work on the basis of pay-per-use, others have a subscription model, and others use a hybrid form that combines fixed and variable costs. One-off implementation or consultancy/training costs are also common. Regardless of the different cost models, the most important factor affecting costs is the transaction volume. It is therefore wise to assess the expected transaction volume per type of service for your PSD2 opportunity before engaging with an API connectivity provider.

6. Organisation-specific requirements

As no two organisations are alike, your organisation may have specific requirements with respect to issues such as data protection, security, user experience, degree of control, risk management and compliance. It is important to identify these specific requirements and ensure that your API connectivity provider is able to meet all of them.

Innopay can help you select the right api connectivity provider

Partnering with an API connectivity provider can greatly accelerate the development and time to market of your PSD2 opportunity. INNOPAY can help you find the API connectivity provider that best fits your needs.

INNOPAY has extensive cross-sectoral experience in enabling organisations to reap the full potential of the opportunities enabled by PSD2. Our consulting services range from defining PSD2 strategies and identifying actionable business opportunities, and selecting the most suitable API connectivity provider for them to assisting organisations with obtaining their PSD2 licence and developing their propositions.

Authors

Luc van Oorschot and Annabel Keulen

ORIGINAL BLOG

GET IN TOUCH

BLOG

Three must-do actions for banks to achieve relevance in the data economy

8 October 2020

Mounaim Cortet

Maarten Bakker

In today's data economy in which everything has become a transaction, future relevance for banks is no longer based on payments alone. To help senior executives of banks to start leveraging their Open Banking capabilities in this context, we recommend three must-do actions to holistically address the components of a digital trust infrastructure (digital identity, consent management, payments and data sharing). These actions will enable banks to build much-needed customer relevance, credibility and trust in the digital transaction era.

Payments has historically been an important anchor product for full-service banks to create customer relevance. However, the introduction of PSD2 has brought with it a real threat of increased pressure on that relevance from third parties who succeed in introducing new, value-added products and services. PSD2 has also required banks to develop new technological and operational capabilities (e.g. digital identification, authentication, API infrastructure, developer platforms, support, etc.) and enhance existing ones that can be leveraged in pursuit of new business models in the Open Banking domain.

It is only natural that many banks are initially focusing on their payments strategy and roadmap. They are keen to better understand how the foreseen payment products under the European Payments Initiative (EPI) fit with existing payment solutions and the possible implications of related developments such as payment initiation services under PSD2, Request to Pay and other value-added payment functionalities enabled through Open Banking. Nevertheless, we are keen to remind banks that the newly acquired capabilities can also be used to gain new relevance in an open data economy in which customers are in control of what data is shared from which sources and for which purposes.

Regulatory reforms such as PSD2, Open Banking and GDPR as well as developments such as the EU Data Strategy and the digital finance strategy are democratising access to data assets across the whole economy. In a changing world in which data is emerging as the new global currency and digital transactions are at the heart of everything we do, customers are becoming more aware of the value of their data assets; they want to leverage their data beyond the platforms and organisations that store it in order to tip the 'data-benefit balance' back in their own favour. This is driving customer demand for increased transparency and control over their data assets – a concept that is also known as 'data sovereignty'.

In our previous article we shared our perspective on the future role of banks as data custodians and the underlying beliefs that bank executives should embrace in order to initiate their sustainable transformation. Banks embracing these beliefs have recognised that putting customers in control of not only their money but also their data is strategically and commercially imperative for future relevance.

Three actions to take right now

To define a solid strategic roadmap that will guide their bank's digital transformation, executives need to initiate these three actions:

1. Shape the strategy and aim the role

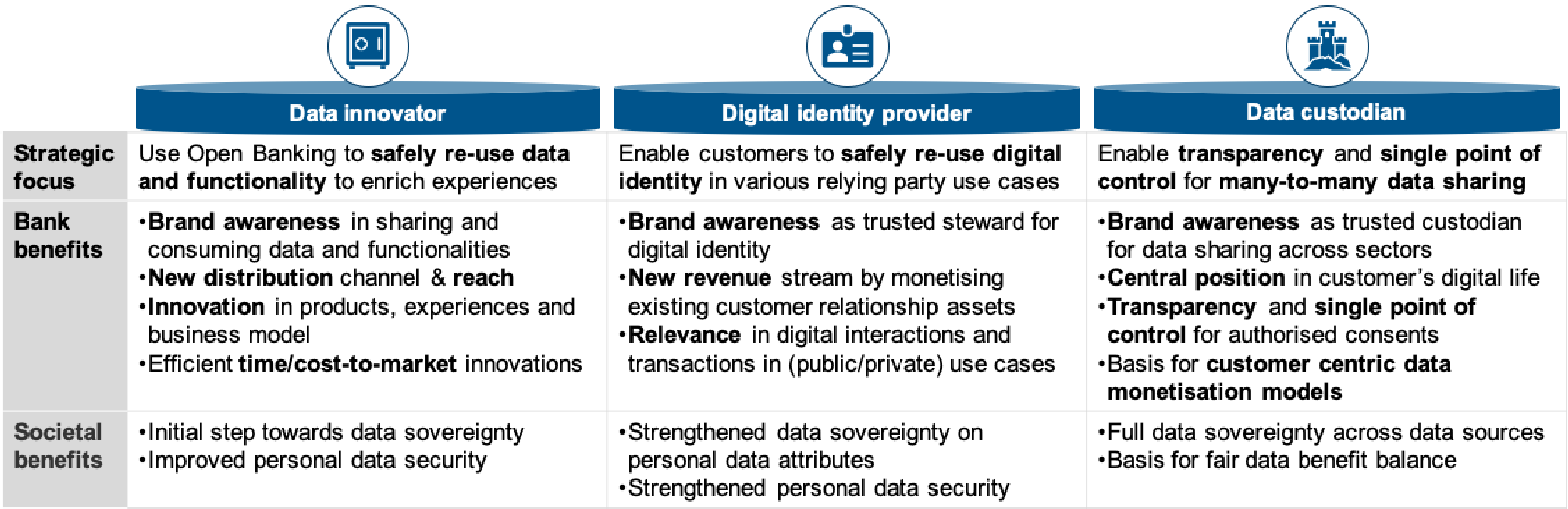
At the heart of the digital trust infrastructure, there are various transaction-based business models and related disruptive growth opportunities that offer significant monetisation options for banks. Three roles in particular will enable banks to secure relevance in the data economy (see Figure 1).

Firstly, banks need to firmly position themselves as a data innovator. This relates closely to banks' strategic Open Banking initiatives (beyond regulatory compliance, e.g. PSD2, CDR) and focuses on enabling and educating their customers to safely re-use data and functionality in other environments. This entails banks opening up their APIs so that their services and products can be embedded in other platforms ('banking as a service') and making use of other APIs to enrich their own digital channels, products and services ('banking as a platform'). This initial step is necessary to lay an effective foundation for new partnerships and business models, and banks must get this step right in order to pave the way for data sovereignty for their customers.

In addition, banks need to focus on positioning themselves as a digital identity provider. By enabling customers to re-use their existing digital identities in relevant relying-party use cases, banks leverage their KYC assets and SCA solutions effectively to shape new revenue streams and increase brand awareness and visibility. With this, banks empower their customers to exercise a concrete form of data sovereignty while also counteracting Big Tech moves in the digital identity space. Banks can actually explore digital identity-related business opportunities in parallel with the first step of becoming a data innovator. Several leading banks are already exploring API-enabled identity services as part of their Open Banking strategy (e.g. CapitalOne, Deutsche Bank).

Besides these two steps, banks can evolve towards becoming a data custodian, leveraging the trusted position it creates by engaging in Open Banking and digital identity. For more insights, see our previous article.

For bank executives, the focus should be on developing a solid understanding of these different roles and the propositions already offered by other players. Based on this, they need to define a common understanding of the vision and strategy



	Data innovator	Digital identity provider	Data custodian
Strategic focus	Use Open Banking to **safely re-use data and functionality** to enrich experiences	Enable customers to **safely re-use digital identity** in various relying party use cases	Enable **transparency** and **single point of control** for **many-to-many data sharing**
Bank benefits	•**Brand awareness** in sharing and consuming data and functionalities •**New distribution** channel & **reach** •**Innovation** in products, experiences and business model •Efficient **time/cost-to-market** innovations	•**Brand awareness** as trusted steward for digital identity •**New revenue** stream by monetising existing customer relationship assets •**Relevance** in digital interactions and transactions in (public/private) use cases	•**Brand awareness** as trusted custodian for data sharing across sectors •**Central position** in customer's digital life •**Transparency** and **single point of control** for authorised consents •Basis for **customer centric data monetisation models**
Societal benefits	•Initial step towards data sovereignty •Improved personal data security	•Strengthened data sovereignty on personal data attributes •Strengthened personal data security	•Full data sovereignty across data sources •Basis for fair data benefit balance

Figure 1: Roles in which banks can secure relevance in the data economy

which is complemented by inspirational use cases and high-level benefit cases. This should then be used to inform decision-making about the bank's preferred role.

2. Select business opportunities & partners

Next, executives need to identify the most viable business opportunities within their bank's preferred role. This entails developing more detailed value cases to prioritise opportunities worthy of further pursuit. Potential partnerships need to be identified to enable and/or accelerate the realisation of each selected opportunity.

3. Define must-win battles & roadmap

For the prioritised business opportunities, the subsequent task for executives is to identify, assess and prioritise key must-win battles and capabilities to prepare for successful execution. Besides this, a clear roadmap needs to be defined that outlines key activities and milestones for execution of the strategy and prioritised opportunities.

Successful participation

Executives at any bank wishing to participate successfully in the data economy will need to perform a review of their strategy and business model as well as their technological and operational capabilities. This starts with developing a solid understanding of how the data economy is evolving, their own vision, strategy and role within the digital trust infrastructure, and the necessary partnerships to enable or accelerate the execution of their strategy. To discuss how these three must-do actions can help your bank to achieve relevance in the data economy, feel free to contact Mounaim Cortet for no-obligation advice.

Authors

Mounaim Cortet and Maarten Bakker

ORIGINAL BLOG

GET IN TOUCH

BLOG

Central Bank Digital Currencies: Today’s buzzword, or time to get ready?

6 November 2020

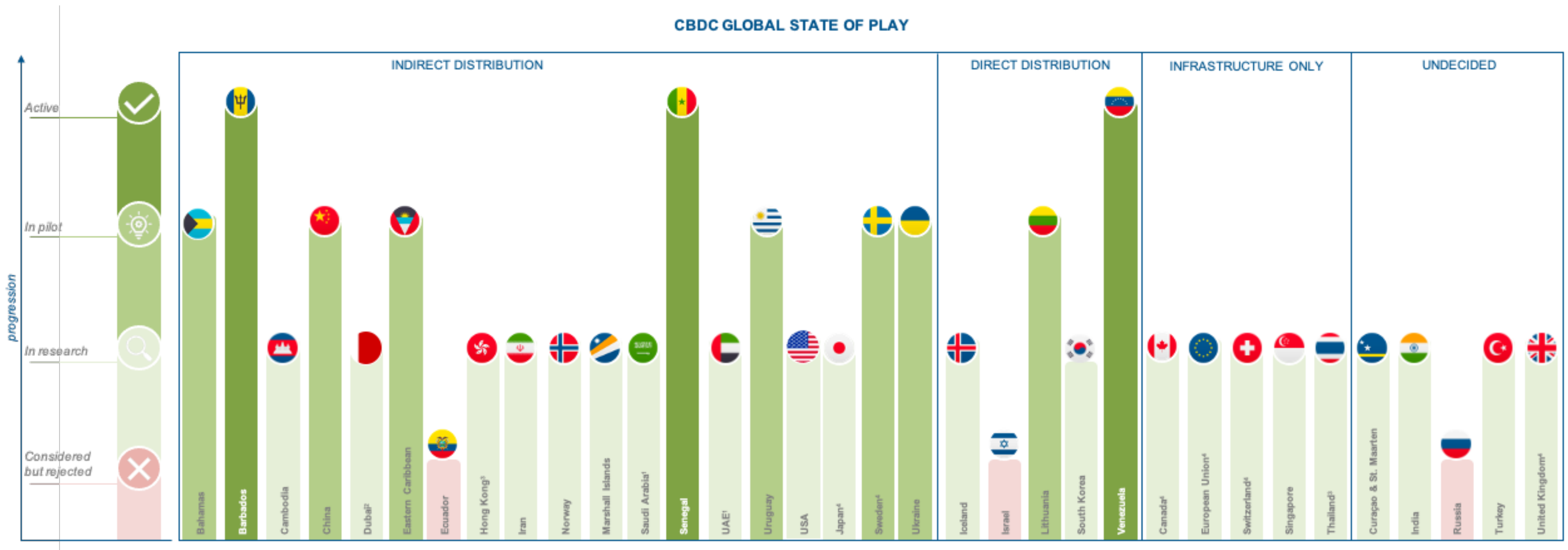
Luc van Oorschot

Pieter Schuurmans

A much-discussed (and much-hyped) topic among central banks is the issuing of currency in a digitalised form: a Central Bank Digital Currency (CBDC). It is claimed that CBDCs could have a significant impact on the payment infrastructure and ecosystem because they could change the rules of the game. However, the various existing CBDC implementations reveal numerous overlaps with the current payment infrastructure, and CBDCs can still develop in many directions. The potential future scenarios and practical implications for the positioning of payment industry players, whether they are payment-focused banks or other payment service providers (PSPs), are therefore unclear. So the question is, what CBDC-related action should payment players undertake today?

Three distinct implementations are being explored

Central banks are considering CBDCs as a reaction to several developments in the payments landscape, such as declining cash use, the growing number of decentralised currencies and private initiatives such as Libra. Currently, only three countries have an active CBDC (see Figure 1), while 28 other countries are further exploring the topic and are in either a research phase or a pilot phase. A further three countries have explored CBDCs and have since decided not to pursue the topic.



Source: INNOPAY Analysis, September 2020

Figure 1: an overview of the current global state of play of Central Bank Digital Currencies (September 2020)

There are currently three ways in which central banks can issue a digitalised currency:

1 Indirect distribution: The central bank offers its digital currency to consumers through banks or other intermediaries. The dynamic of this approach is similar to how cash and scriptural money currently works. It implies a positioning of payment players that is similar to today's positioning.

2 Direct distribution: The central bank offers its digital currency directly to consumers. This approach is similar to current cryptocurrencies such as bitcoin with a decentralised storage of value, or to a payments account directly with the central bank. However, this option raises questions regarding consumer security, as additional security services (e.g. two-factor authentication) are expected to be required. These services are unlikely to be provided by central banks, but rather by other types of (licensed) service providers, effectively making it similar to an indirect distribution model. Given the security considerations, this model implies a positioning of payment players that is largely similar to today's positioning. This conclusion is supported by the recent joint publication by seven central banks and the Bank of International Settlements (BIS).

3 Infrastructure only: The central bank offers its digital currency to banks or other financial institutions only, for use in interbank payments and securities transactions. In practice, this would create a payment infrastructure specifically for banks that is an alternative to existing settlement systems rather than being a consumer-facing system. Infrastructure-only CBDCs seem mostly relevant and impactful for developing economies with a need for more efficient interbank systems.

Further maturing required to determine impact

Although the topic of CBDCs is gaining traction, especially in the media, the disruptive potential of CBDCs for payment players currently seems limited because the various CBDC models are either comparable with existing practices, unlikely to occur due to security considerations or too narrowly focused. However, since the topic of CBDCs is currently still in its infancy, there is uncertainty about its final shape. This uncertainty is reflected in the BIS publication, which raises questions about features and criteria for CBDCs. Matters such as the level of standardisation, interoperability, centralisation, required security, and whether CBDCs will be monetisable, consumer-facing and cross-border-enabled all need to be explored much further. These issues could increase the potential of CBDCs to disrupt the current positioning of payment players. However, since it will take some time for the topic of CBDCs to mature, it seems too early for payment players to incorporate CBDC initiatives into their short-term actionable strategies.

Three imperatives for payment leaders

Nevertheless, as all three CBDC models could have an impact on payment players, albeit to varying degrees and depending on the level of maturity of each model, we advise payment players to start taking action today. Whether they are keen to be among the leaders and innovators, want to engage as fast followers or prefer to wait until the market is more mature, it is important that payment players already spend time on understanding how emerging CBDC models will impact the payments landscape in general and their business in particular. To begin shaping their strategic perspective, payment players should initiate the following three actions:

1 Closely monitor evolving design choices and results of existing CBDC initiatives (e.g. China's DCEP and Sweden's e-Krona)

2 Define future scenarios and assess how each scenario can impact their current role across markets.
3 Actively shape the future of CBDCs in their region together with their central bank by actively engaging with them on the topic and, optionally, start collaborating with other banks or PSPs to shape the future together.

Innopay is closely monitoring the evolution of cbdcs

Based on our experience and vision of the evolution of the payments market, INNOPAY can help you with the next steps in preparing for the future impact of CBDCs. Our consulting services range from defining actionable CBDC strategies and identifying actionable opportunities, to assisting in dialogue with other market players and central banks.
Reach out if you are interested in finding out how you can ready yourself for the future impact of CBDCs
This blog was written in collaboration with Krijn Reijnders.

Authors

Luc van Oorschot and Pieter Schuurmans

ORIGINAL BLOG

GET IN TOUCH

BLOG

Why we Need a Data Exchange Board to Improve the EU Data Governance Act

9 December 2020

Data Sovereignty Now

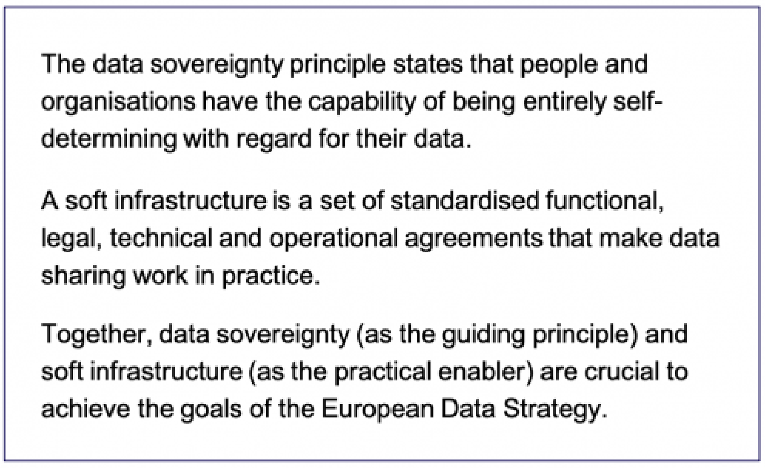
In this blog, aNewGovernance, iSHARE, INNOPAY, International Data Spaces Association, Meeco, MyData Global, SITRA and The Chain Never Stops - eight organisations of the Data Sovereignty Now movement – explain why the recently published proposal for the EU Data Governance Act is a very good step forward. They also outline their suggestions for further elaboration in order to accelerate the development of a governance framework that will provide true control over personal, business and public data.

Supported by the European Data Strategy, the EU is striving to create a digital single market for the data economy and data sharing that benefits society as a whole. This will be based on European 'data spaces' that allow data to flow freely within the EU and across sectors whilst staying true to EU values such as privacy, transparency, self-determination, security and competition.

As part of implementing the data strategy, the European Commission published its proposal for a regulation on European data governance, known as the Data Governance Act. As member organisations of the Data Sovereignty Now (DSN) movement, we applaud this proposed legislation because it contains several essential elements for enabling data sovereignty, including:

- People, businesses and public-sector bodies should have control over data about them.
- Data and data spaces need to become interoperable across sectors.
- Recognition of current and future data intermediaries (called 'data sharing services' in the regulation) such as data operators, gateways and platforms within data ecosystems.
- Balanced pan-European governance, under the leadership of the so-called Data Innovation Board.

The data sharing services or data intermediaries have to comply with still-to-be-defined binding requirements. Once created, the requirements for data sharing services will offer a basic level of compliance, legal conditions and last but not least a unified and inclusive data experience across data spaces, for all people, businesses and governmental users of data services. The data intermediaries thus ensure that the rights of data subjects (in case of personal data) and other rightsholders are respected and that people, businesses and governments in the various data spaces are empowered to re-use data about themselves.



The data sovereignty principle states that people and organisations have the capability of being entirely self-determining with regard for their data.

A soft infrastructure is a set of standardised functional, legal, technical and operational agreements that make data sharing work in practice.

Together, data sovereignty (as the guiding principle) and soft infrastructure (as the practical enabler) are crucial to achieve the goals of the European Data Strategy.

Figure 1.

Hidden gem: Data Innovation Board

Chapter VI of the proposed Data Governance Act mentions the establishment of a Data Innovation Board that will assist and advise the Commission on the strategic matters in data governance, such as enhancing interoperability and developing the actual requirements applicable to data sharing providers. We regard this Data Innovation Board as a 'hidden gem' in the proposed regulation since it could act as a launching pad for many critical developments of soft infrastructure in the future. Furthermore, in our view, the Data Innovation Board – with its strategic focus – should be complemented by another governance body focusing on the more tactical and operational aspects of enabling data sharing and interoperability in practice. This combination of strategic guidance and operational efficiency would ensure accomplishment of the real aims: to create trust in data sharing, and to co-create, organise and stimulate adoption of decentralised access to and exchange of data while maintaining transparency, security and interoperability.

This operational governance body could be called the Data Exchange Board. It should be tasked with agreeing upon the initial requirements for the data sharing services and updating the requirements going forward, driven by the needs of people, markets and public-sector use cases. We recommend building upon the existing science, research and practical experience from interoperable data sharing (e.g. IHAN, IDSA, Data Sharing Coalition, iSHARE and MyData Operators, to name but a few) and merging best practices to organise this on a pan-European scale. The Data Exchange Board would create the living link between the aims of the regulation and the means and best practices that are emerging in the real-life use cases. We believe that this connection will be essential to drive large-scale adoption of the data sharing services in the coming decade.

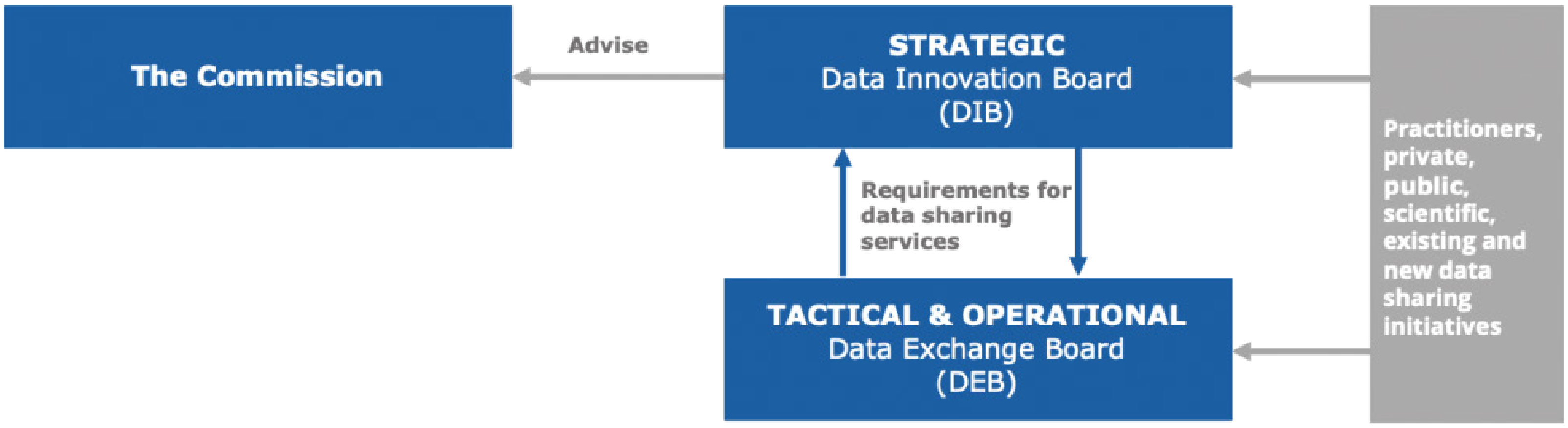

The Commission
Advise
STRATEGIC
Data Innovation Board
(DIB)
Requirements for data sharing services
TACTICAL & OPERATIONAL
Data Exchange Board
(DEB)
Practitioners, private, public, scientific, existing and new data sharing initiatives

Figure 2: The relationship between the strategic Data Innovation Board and the proposed operational Data Exchange Board, with the European Commission on one side and the practitioners on the other.

Conclusion

We believe that the European data governance framework must be designed to establish and provide continuity to the soft infrastructure for data sharing. The still-to-be-established Data Innovation Board will be elemental in achieving this aim. We recommend that this should be further complemented by a Data Exchange Board that will focus more on the tactical and operational level, both in the sunrise of the soft infrastructure and in the future operational growth and innovation phase of the decades ahead.

Our vision on the key steps to achieve data sovereignty through soft infrastructures:

1. Soft infrastructure for data sharing: Develop functional, legal, technical and operational agreements that support the most pressing use cases of people, businesses and governments in the various data spaces.
2. Based on existing best practices: Much of the groundwork on soft infrastructure for data sharing has already been done in the past decade by researchers and business practitioners around the world. The initial version of the requirements for data sharing services should include these best practices.
3. Living form of standardisation: The soft infrastructures are a living form of standardisation and should be allowed to evolve over time; the common way of dealing with data must continuously respond to market needs and applications.
4. Operational governance: To include the best practices from the practitioners and enable the continuous evolution of the standardisation, a sound governance model should be set up which represents public-sector, private-sector and people's interests.
5. Initial implementation: The organisations that have created the agreements should roll out and implement the first version of the soft infrastructure. This will provide referenceable integrations and, importantly, validate market adoption.
6. Roll-out and adoption: The soft infrastructure should then be extended across all sectors over the coming decade.

We are keen to start the dialogue with policymakers and politicians to achieve this together. Feel free to contact us for more details or to reflect on or discuss how a governance framework can help to achieve data sovereignty and advance the European digital economy.

Author

Data Sovereignty Now

ORIGINAL BLOG

GET IN TOUCH

BLOG

Top 3 think outside-the-box ideas emerging from Central Bank Digital Currencies

12 December 2020

Luc van Oorschot

Pieter Schuurmans

Over the last five years, most payment innovations have focused on improving customer interfaces, without fundamentally changing the payment instruments used. Digitalisation is about to change these for good.

Latest trends such as embedded finance, dedicated marketplaces with embedded payment and billing, decoupling shopping from physical locations, a rise of digital wallets, and Super Pay Apps usage have made the act of paying has become less visible and increasingly dematerialised and disintermediated. Forward-thinking ecommerce/payments companies have already started to offer disruptive payment solutions such as crypto assets (including stable coins), based on encryption and distributed ledger technology (DLT). The COVID-19 pandemic has further reinforced the shift to digital payments and confirmed the importance of safe, accessible, and convenient (including contactless) payments for remote and face-to-face transactions.

This is the backdrop against which digital money – stable coins, e-money, CBDC, cryptocurrency - have emerged. Central bank digital currency (CBDC) has the potential to increase payments diversity, encourage financial inclusion, support cross-border payments, assists with payments digitalisation in general. At the moment, central banks provide cash, used by the public, and electronic payment services, used by eligible financial institutions. However, since 2015 when Andrew Haldane, the UK central bank's chief economist back then, suggested that a digital currency based on Bitcoin could alleviate monetary policy problems and that paper money be banned entirely, there has been a growing conversation about whether central banks should offer a digital version of cash. When that will happen, how can digital cash be leveraged to support innovation?

1. **Welcoming intelligent services via embedded finance**
   Based largely on the use of technology, embedded finance refers to the integration of financial services into other (non-financial) services and experiences. It enables brands to focus on solving the problems of their customers with real-time, intelligent (e.g., alert me when I've been paid or get paid early), and context-aware experiences. In a nutshell – Uber (Uber has disrupted the taxi industry by integrating payment functionality directly into its app to reduce ride-payment friction for drivers and passengers). This concept is strongly connected with Open Banking and Open Data economy, which encourage a natural flow of data between consumers and businesses, with proper data protection and consent management methods in place, for the benefit of all parties involved.

   CBDCs maintain an electronic history of transactions (what the consumer buys, where, and when), drawing a full picture of his/her preferences and savings behaviour. If this data-trace is recorded and analysed, based on proper privacy and protection strategies, it can offer enormous advantages to the data's owner. Innovative and sustainable ideas such as green banking – calculating users carbon footprint; healthtech - calculate probabilities of getting some diseases due to extra consumption/or lack of consumption of certain foods; mobility – calculate the best transportation route to take, considering what matters for a consumer/tourist going somewhere (travelling costs vs. environments costs vs. health impact), etc can be built. Relying on this opening of (payment) data, in April-May 2020, many fintech's were involved in distributing COVID-19 stimulus payments. Similarly, a CBDC could enable governments to directly stimulate the economy down to every citizen through 'helicopter money', as INNOPAY's Douwe Lycklama mentions. Recognising the success of these initiatives, it is hoped that in the US, a tech-forward government administration will rely more on neobanks/fintechs/CBDCs/helicopter money to distribute funds allocated in future stimulus packages.

2. **The merits of programmable money**
   Programmable money is real money represented in digital form. Also known as tokens, this digital currency is tracked with corresponding electronic ledgers (e.g., blockchain) which record the transaction that is publicly and securely shared. To promote sound governance and to keep the programming interfaces equally available to banks and other participants, this ledger should preferably be based on open-source software, according to IBM. Bitcoin is one of the most famous digital currency, however, it was met with many critics from the banking sphere due to its volatility and its possibility to disintermediate the middleman (e.g., banks, custodians, and other types of trustees). As such most banks see cryptocurrencies as a risk to their clients, and a potential threat to their business model.

   However central banks have started to ponder over the innovation digital money promise for businesses and end consumers and have been quietly but actively evaluating their benefits and experimenting with their versions, called CBDCs. In 2019, 70% of central banks acknowledged they are studying the issue, with about a quarter saying they already have the authority to issue a CBDC or will soon have it, though 85% of central banks say they are unlikely to issue a CBDC within the next three years, according to a paper issued by BIS.

   A CBDC designed to allow for programmability could enable automated execution of certain operations, such as payment of interest, setting spending goals on budgets, or triggering tax collection. The latter will reduce today's cash-driven informal economy and cut on tax evasion, while the other functionalities influence its application. Still, while analysing the potential benefit that a CBDC could provide in the context of existing payment mechanisms, the FED agreed that "while current RTGS systems do not have the same level of programmability built into their platforms that some distributed ledgers have, RTGS systems could achieve similar results through application programming interfaces (APIs)".

3. **Solving the digital identity dilemma**
   Undoubtedly the most controversial money project of 2019 and 2020 has been Facebook's Libra (currently rebranded as Diem). Criticism and negative responses towards Libra were unlashed due to the risk it poses to global financial

stability. Still, "Libra payment system [aims] to integrate smoothly with local monetary and macroprudential policies and complement existing currencies". Furthermore, Libra Association (now rebranded Diem) hopes to be able to collaborate with central banks on issues such as the integration of the Libra payment system with CBDCs.

Libra's innovative potential goes beyond payments. According to David Birch, Facebook's most interesting effort is its plan to create a digital wallet, Novi, which much more disruptive potential than the currency basket that they are proposing for it 'because the global problem of financial inclusion has much more to do with identity than it does with money'.

As providers of electronic payment services must comply with AML, BSA, KYC, and electronic recordkeeping requirements, a CBDC/Libra would almost certainly need to comply with these regulations. As Facebook has access (with users' consent) to lots of info about you, standardising some of the things included in the Novi wallet such as proof of age, financial services passport, trusted traveller status, and loyalty cards will deliver global benefits by bringing trade to hundreds of millions more people than the banking system has been able to.

Now the headlines are made mostly by central banks discussing, testing, analysing CBDC, with a strong focus on offering innovative payment solutions that work both offline and online, within and across national borders. But the possibilities are endless, and I encourage you, the reader, to be bold, creative, and join the conversation about what digitalisation means. Still not convinced? Here is a small paragraph I took from an interview with the authors of best-selling management book 'Everything Transaction', Shikko Nijland, Douwe Lycklama, and Chiel Liezenberg.

> When studying platforms, we found that there is little imagination about what comes next in our digital economy. Leaders, politicians, and the press are all very busy amplifying the threats, worries, and pitfalls of platforms, AI, and big data, but little solutions other than 'we need more rules'. In the book, we pay attention to the strategic aspect of collaboration between platforms […] such strategies required specific leadership and a longer-term version than the length of a typical C-level job period.

Like this story? To learn more about CBDCs, the innovation they promise, and the implications and risks they pose, download The Payper's eBook Central Bank Digital Currencies for Dummies – A Quick Guide into CBDCs.

Authors

Luc van Oorschot and Pieter Schuurmans

ORIGINAL BLOG

GET IN TOUCH

BLOG

Why banks must evolve their operating model to capitalise on the commercial opportunities of Open Banking

12 December 2020

Josje Fiolet

Mounaim Cortet

In this blog, Josje Fiolet and Mounaim Cortet, Senior Managers at INNOPAY, discuss how banks need to update their ways of working to realise the commercial benefits of Open Banking. They provide an introduction to the six main challenges for banks and propose a targeted approach to help them improve their operating model in three key areas.

To receive exclusive access to the extended Paper, which discusses these issues in more detail, readers are invited to download our paper 'Executing Open Banking at scale and speed requires a supporting operating model'.

DOWNLOAD

Leveraging open banking at scale and speed depends on integrating key activities within the bank's daily operations

Open Banking is a key strategic component as banks look to secure their future relevance in the digital economy. However, many banks have been slow to recognise the importance of fully integrating Open Banking activities within their existing operating model.

Only by fully understanding the new dynamics at play, and then taking the right steps to evolve their current operating model, will banks be able to effectively integrate Open Banking initiatives and teams into their daily operations.

And this integration implies that Open Banking must become a fundamental part of the day-to-day value creating activities of the bank. Continuing to treat it as a standalone domain will not effectively contribute to the bank's strategic objectives. We see six areas which require specific focus.

Six common challenges for banks when integrating open banking activities

From our experience in supporting Open Banking transformations, we observe that six challenges are impeding banks from monetising Open Banking at scale and speed. These challenges closely align with the need to integrate important groups of activities into the existing daily value creation operations of banks.

These six groups of activities include:

1. API proposition development & management
2. API pre-sales & business development
3. API onboarding & risk management
4. API service, support & relationship management
5. API business plan, budgets & incentive schemes
6. API platform capability

For each of the activities, banks need to ask themselves: Are these activities, and the teams that conduct them, fully integrated within the daily operations of the bank?

Integrating each activity comes with a specific set of challenges that we discuss in more detail in the extended Paper. If integration is not managed effectively, banks will be unable to operate Open Banking at scale and speed, and ultimately struggle to deliver on their strategic objectives.

Three operating model elements which will support the integration of these activities

Once the challenges of scaling Open Banking at an activity level are understood, it is possible to identify the required modifications to a bank's existing operating model. Although the operating model is built of many components, we have pinpointed three elements that require particular attention to successfully embed Open Banking.

These three elements are:

- Roles and responsibilities
- Governance & way of working
- Data & metrics

Each bank should consider how the Open Banking activities can be effectively integrated by making adjustments to these three elements of their operating model. The answer will vary based on the particular setup and maturity within each bank. By doing this, it is possible to manage changes in a consistent manner, and to maintain a coherent operating model that ensures efficient daily operations whilst supporting the agreed Open Banking strategy. And since the Open Banking journey has only just started, banks will need to constantly review and refine their ongoing responses to changing circumstances.

INNOPAY has supported several banks in their Open Banking transformation, bridging strategy and scaled execution by establishing a coherent operating model that supports their business objectives.

To further discuss your own case and how we can help you, do not hesitate to contact Josje Fiolet or Mounaim Cortet.

And don't forget, if you would like to access the extended Paper on how to manage this operating model transition, please download our paper 'Executing Open Banking at scale and speed requires a supporting operating model'

Authors

Josje Fiolet and Mounaim Cortet

ORIGINAL BLOG

GET IN TOUCH

BLOG

Securing future relevance in the changing financial system: three strategic stablecoins considerations for banks

22 December 2020

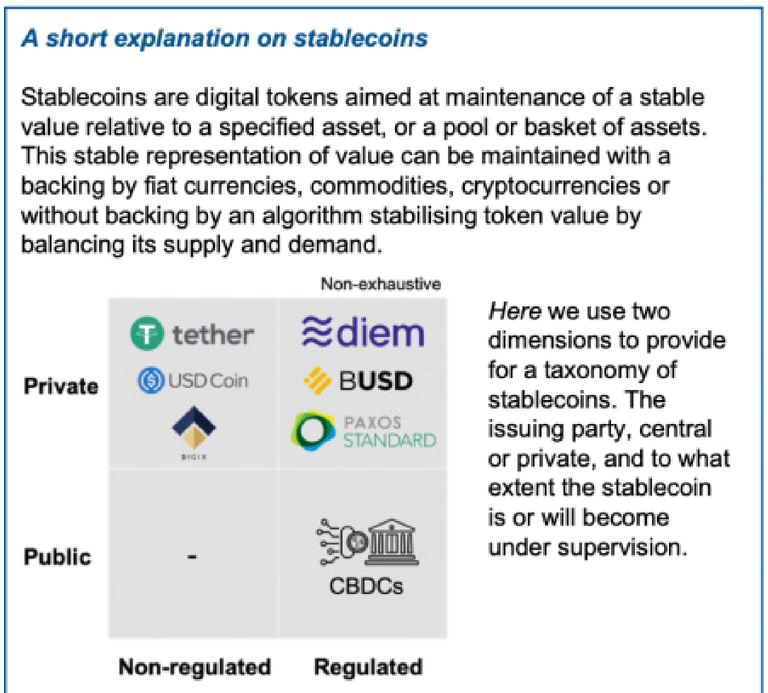
Josje Fiolet

Pieter Schuurmans

Widely regarded as the more respectable face of crypto, stablecoins are poised to become an integral part of the financial system's future. With their ability to stabilise prices and in conjunction with harmonised regulations, stablecoins hold the promise of improving access to financial services. During EBAday 2020 in November, Josje Fiolet, senior manager at INNOPAY, moderated a panel to discuss stablecoins and their potential impact on banks. In this article we build on the insights from that panel and summarise three strategic considerations to help banks position themselves in the emerging market and prepare for the potential impact of stablecoins.

Growing interest in stablecoins

The topic of stablecoins is attracting ever-more attention. The numbers speak for themselves: the market capitalisation of stablecoins grew from approx. US$5 billion in November 2019 to close to US$24 billion in November 2020, an increase of 360% in just one year[1]. Market players, regulators and media companies are becoming increasingly interested in stablecoins, as highlighted by Facebook's Diem (formerly Libra) initiative, the research and development activities relating to Central Bank Digital Currencies (CBDCs) by central banks (see our latest publication), and recently proposed regulations for stablecoins, such as MiCa by the European Commission[2] and the oversight framework by the European Central Bank (ECB)[3]. Figure 1 show a brief explanation and taxonomy of stablecoins.



A short explanation on stablecoins

Stablecoins are digital tokens aimed at maintenance of a stable value relative to a specified asset, or a pool or basket of assets. This stable representation of value can be maintained with a backing by fiat currencies, commodities, cryptocurrencies or without backing by an algorithm stabilising token value by balancing its supply and demand.

Here we use two dimensions to provide for a taxonomy of stablecoins. The issuing party, central or private, and to what extent the stablecoin is or will become under supervision.

Figure 1: Stablecoin taxonomy

The impact of stablecoins on the current position of banks

Stablecoins address the challenges related to price volatility and scalability of the first wave of crypto assets (e.g., Bitcoin, Ripple) to offer an attractive means of payment and store of value. Stablecoins are aimed at providing an alternative real-time payment infrastructure and services with improved efficiency compared to the traditional infrastructure, for example in the field of cost-efficient cross-border payments. As with any type of innovation in payments, stablecoins enable new payment services and new players to enter the market. As pointed out during the EBAday panel, the emergence of large global stablecoin initiatives by Big Techs could undermine the current level playing field in payment services as their established global customer bases allow them to scale rapidly. But it is not only the well-known Big Techs that are aiming to secure a foothold in this rapidly growing domain. The first stablecoins were initiated in 2014 by private parties who had no prior position in the payment ecosystem. For example, Tether is currently the largest operational stablecoin, with an average daily trading volume of approximately US$34.4 billion in October 20201. With central banks around the world now initiating CBDCs too, it is clear that this domain is considered to have huge potential.

With the market developing rapidly, policymakers are looking very closely at the topic of stablecoins and issuing and reviewing regulations to stimulate innovation on the one hand and mitigate associated risks on the other. European policymakers identified various risks that could have implications for the existing financial system and could impact on banks' business models. Due to their potentially large reach and adoption, stablecoins could not only pose challenges to fair competition and the strategic autonomy of the payment system, but could also jeopardise financial stability and monetary sovereignty overall, for example as a consequence of currency substitution[4].

Three strategic considerations to help banks position themselves in the future financial system

Banks still have a dominant position when it comes to offering payment services to businesses and consumers with fiat accounts. In view of the above-mentioned developments, however, banks are urged to reconsider their strategic positioning to turn risks into opportunities and reap the benefits of the changing financial system. These three strategic considerations will help them to do so:

1. **What role do we aim to play in this changing financial ecosystem?**
   The EBAday panel members were united in their belief that banks have a role to play. They pointed out that for example the MiCa regulation is aimed at encouraging banks to interact in the field of stablecoins by framing all kinds of activities. Banks could play a role in facilitating the creation, redemption, circulation and use of stablecoins, for instance. Banks have a competitive advantage since they already have a long-standing trust-based relationship with their customers. They have always been positioned as a 'money custodian', so becoming an 'asset custodian' or 'data custodian' in a broader sense would be a natural extension of this role.
2. **What new propositions can we develop to remain relevant to our customers?**
   Banks can already start developing new propositions by linking their traditional infrastructure to the alternative infrastructure required for stablecoins. For example, they could develop new propositions based on the programmability of stablecoins and CBDCs (e.g. supply chain redesign of invoices, cross-border real-time transactions), provide KYC/AML services to issuers of fiat-backed stablecoins and CBDCs when issued through traditional banks, and/or support stablecoin retail payments. In fact, interoperability of stablecoins with other payment systems is highlighted by the G7 as an important

requirement. With banks having a dominant position in current payment systems, this is a promising field for them to consider

3. **Can we gain a competitive advantage by collaborating?**
Competitive pressure and challenging market dynamics are driving banks together. During the panel discussion, it was pointed out that collaboration among banks is an important asset to consider. There are already various examples of banks working together, such as in the European Payment Initiative (EPI) to launch a new payment system aimed at taking on rival card schemes and the threat posed by Chinese and American Big Tech firms. Overall, there is growing political pressure for banks to collaborate in all kinds of domains related to digital transactions. The EPI was also a response to the ECB's call for more collaboration[5] and, in the recently published Digital Finance Strategy, the EC[6] urges the private financial services sector to be at the forefront of developing and delivering digital identity solutions. Overall, this pressure is aimed at ensuring that Europe retains and reinforces its strategic autonomy in financial services and the broader digital economy. As highlighted in this article, the strong competitive dynamics in stablecoins and the overall payment system could be yet another reason for banks to collaborate in order to retain their competitive advantage. Could the existing infrastructure include stablecoins as well?

Although the market is at a relatively early stage of development and still evolving, banks need to reconsider their position now if they wish to secure future relevance in the changing financial system. We will continue to keep you up to date on all the relevant developments, but please reach out to us if you are interested in discussing in more detail how you can prepare for the future impact of stablecoins.

[1] INNOPAY analysis, based on historical data by CoinGecko
[2] Regulation on Markets in Crypto-assets (MiCa) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593
[3] European oversight framework for Payment Instruments, Schemes and Arrangements (PISA) https://www.ecb.europa.eu/paym/intro/cons/pdf/pisa/ecb.PISApublicconsultation20201027_2.en.pdf
[4] G7 paper working group on stable coins https://www.bis.org/cpmi/publ/d187.pdf
[5] https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200702~214c52c76b.en.html
[6] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

Authors

Josje Fiolet and Pieter Schuurmans

ORIGINAL BLOG

GET IN TOUCH

INTERVIEW

Digital Trust Challenges and Opportunities

3 February 2020

Jelger Groenland

The Data Sharing Days 2020, Europe's premier data sharing event that took place from 27-28 January 2020 in The Hague, The Netherlands revolved around the theme of 'Data sovereignty'. We spoke with Jelger Groenland, digital trust & security lead at INNOPAY, who advises clients on challenges and opportunities arising from the digital transformation. We talked to him about the importance of trust in today's digital transactions era and the role of cybersecurity.

How does digital trust relate to data sovereignty, the theme of the Data Sharing Days that INNOPAY co-hosted?

Data sovereignty and digital trust are very closely linked. The concept of data sovereignty – an individual's full right and control over their own data – is becoming a prerequisite to build trust with customers in the digital economy. Consumers need to have full control over their personal data in order to trust a business. We're increasingly seeing companies providing more transparency about their privacy policies and what it means for their customer. They are also giving customers the tools to manage their own data. We expect this will increasingly become the norm. It can also create a competitive advantage because consumers are ever-more aware of their privacy and concerned about how their data is being used.

What recent challenges and dangers have been illustrated frequently in the aspect of cybersecurity?

Financial crime and fraud are attracting growing attention in the context of digital transactions. Attacks frequently happen through e-mail phishing and so-called 'smishing' (phishing via text message). In such cases, consumers are tricked into giving away their credentials to criminals because they believe they are interacting with a trusted party, often their bank. This is one reason behind the decline in digital trust, and as an industry we need to reverse this trend if we are to tap into the full potential of the transactional internet. Although I don't believe this problem can be solved overnight, moving to a more sophisticated trust infrastructure for digital transactions – a data-sharing scheme that provides seamless authentication without passwords, and in which the data owner retains control of their data at all times – could drastically reduce such risks.

Another challenge is the fragmentation of the digital transaction value chain. In the banking industry, for example, the PSD2 regulation and open banking have resulted in many – often new – players taking ownership of part of the customer journey for payments and related services. For customers, this means new brands and apps are requesting their financial and personal data. As a consumer, how do you differentiate between a trusted app and a malicious one? It's becoming increasingly difficult. To tackle this, we need mechanisms that allow businesses and consumers to interact on an infrastructure of trust. There is a similar shift towards openness in other industries too, which is making it even more important to have a cross-industry trust infrastructure in place.

What models or operational mechanisms would INNOPAY advise to their clients to utilize in case of a cyber attack or data leak? For instance, do standard procedures and protocols exist for such matters that have demonstrated concrete effectiveness?

A quick and adequate response to an identified data breach has a direct impact on the costs. Several studies in the insurance industry have identified this relationship. The same goes for the time it takes to actually uncover infiltration and malicious activities. Sometimes an attacker can have access for months before they are discovered. The sooner a compromise is detected, the better in terms of the costs and the damage.

So what should organisations do? Well, they obviously need a robust response capability. This is typically assigned to a Security Operating Centre (SOC) or response team, but it can be outsourced too. In addition to a technical response capability, organisations should assess and manage the system for issuing notifications to regulators and customers – either by handling it themselves or outsourcing it to experienced partners.

Managing the reputational damage and loss of trust is a bigger challenge. We always recommend organisations to think about this and include it in their digital trust strategy. Typically, this means providing transparency to everyone involved and being clear about what steps you are taking to put things right. Ideally, organisations should have a Chief Trust Officer to prepare and coordinate this response across departments.

In what areas does room for improvement or development exist on the security surface?

Everyone in the industry is aware of the growing cyber threat as criminals become more professional and the size of the enterprise's potential attack surface increases. However, what still surprises me is the mainly operational-technical approach to cybersecurity. This has led to a situation where there are simply too many systems to protect, too many vulnerabilities to patch, too many tools to work with and too few specialists available. The conversation is often about tooling instead of more fundamental strategic questions about data sovereignty, data retention strategies and transforming the technology landscape to reduce risk for the enterprise.

Although data is regarded as 'the new oil', there is a large potential downside when data is compromised. Storing too much data without a clear business case has actually become a liability. This is more commonly acknowledged in the payment industry, where businesses typically try to limit their exposure to data as it obligates them to be PCI DSS compliant. In this industry parties prefer to avoid the burden and costs of compliance by outsourcing payment processes and only decide to do this themselves if absolutely necessary. So there is still much room for improvement in terms of a strategic approach to customer data.

What do you see as your biggest future challenge concerning security and privacy issues in the digital transactions business?

At INNOPAY, the biggest challenge we see is to unleash the true potential of the transactional internet – and that means breaking out of the trust paradox. This refers to two seemingly opposing needs: to make user data –- and in particular personal information – more accessible, while at the same time improving data security and hence securing users' trust in further digitisation. Recent data scandals indicate just how fragile that trust is and how easy it is for privacy concerns to grow. It is possible to break out of the paradox by moving from institutional trust towards infrastructural trust. Ideally, users have possession and control over their own (identity) data and trust should be embedded in the internet itself.

How are trust and cooperation developed between companies? Through which models and operations is trust gained, considering this is a vision INNOPAY has as a sustainable solution for digital transactions? In that regard, it could be noted that the protection of privacy plays a pivotal role.

In the current landscape, online cooperation is based on one of two dominant models. The first is through bilateral transactions between two parties. Although this approach is flexible, the biggest problem is that it does not scale. The second model is through online platforms. This is an efficient way to scale many-to-many transactions, but it has several major drawbacks, the biggest one being that benefits and governance are centralized with the platform owner. This puts users of the platform at a disadvantage and poses a major risk to their business continuity. Another drawback is that this model promotes data siloes which hinder innovation in the long run. Therefore, INNOPAY proposes a third model, which we call 'Trust Schemes'. This model is not only scalable, but is also based on a distributed model of control and collaboration. Trust Schemes are founded on agreements relating to a wide array of standards for the exchange of data and information. These address technical aspects, but also organisational, legal and operational perspectives of collaboration.

ORIGINAL INTERVIEW

GET IN TOUCH

INTERVIEW

'Growing an entire transactional ecosystem in Asia based on an inclusive, collaborative approach'

30 April 2020

Josje Fiolet

When Josje Fiolet started at INNOPAY around six years ago, the transactional world was completely new to her, but she was intrigued by the opportunity to work in such a dynamic and ever-evolving industry which combines business, regulatory and technical aspects. Since then, on the company's fast-track talent programme, she has progressed to the role of senior manager, with a focus on leading client projects related to digital identity, data sharing and payments. Here, she talks about a recent project in southeast Asia.

Who was the project for?

As a 'for purpose' company rather than a 'for profit' one, our client is closely interwoven in the Asian country's payments landscape. It is involved in developing payments products and services together with industry players, but it also operates infrastructure such as the ATM network and payments systems. Moreover, it plays a role in realising the objectives of the country's ten-year blueprint for the financial sector. The client was actually a consortium of stakeholders, with the participating organisations ranging from local, national and foreign banks in all shapes and sizes to non-banking participants such as third-party acquirers and FinTechs.

How did INNOPAY first get involved in the project?

We were initially recommended for the project by the Dutch Payment Association (DPA), which heard about our client's plans through its participation in an international association for similar interbank organisations worldwide. We have worked with DPA quite often in the past, such as when supporting the development of the iDEAL online payment scheme for the Dutch banking industry. In fact, Australia is another member of that association and we've also successfully supported AusPayNet in the past, so we actually got recommended from two sides! Once we were on the shortlist, the client soon realised that – despite us not having an office in Asia – we were the natural choice as the worldwide leader in payment schemes with the most experienced consultants. We later heard that another deciding factor was our unique collaborative approach to co-creation combined with our transparency about which aspects we needed to take care of ourselves to maximise the value, and which parts of the project could be handled by local partners with our support.

What did the project actually entail?

Our client is aware that, to enable a digital economy, it is essential to advance the payment landscape towards 'digital first' or cashless. But in the client's country, an estimated 95% of all retail transactions are still based on cash and cheques. Therefore, as part of the country's ten-year blueprint, our client is keen to accelerate the shift to a digital transactional ecosystem by adopting e-payments. Our brief was to develop a vision and adoption plan for the next three years. We started on the preparatory work in October 2019, and then in early November a team of three of us flew to the country to work on-site. We were supported by a regular team of four back in the Netherlands, plus specialised subject-matter experts who flew in and out for important touchpoints with stakeholders as necessary.

We started off by conducting a thorough assessment of the current payments landscape in the country and elsewhere. We identified best practices in various different countries, including Sweden, Singapore, Canada and Australia as well as the Netherlands, and analysed how they could be applied in the local context. We also held lots of interviews and meetings with all types of stakeholders, from CEOS of major banks to FinTechs, to develop a shared vision and shape the story together. Our discussions covered how the world of payments is evolving and what our client could expect in the future – including the exponential growth of digital transactions and how payments are at risk of becoming a commodity. Looking a step further, we also touched on the ever-increasing importance of digital identity, privacy and data control, and the role of financial institutions in such services. By considering recent developments elsewhere, such as the European Data Strategy and the link to data sovereignty, our client is in a position to benefit from 'leapfrogging'… to see where the world is heading and get it right first time by fully embracing the possibilities of the digital transaction era.

What was the biggest challenge in the project?

This was an interesting case because the local market actually already has a large variety of relatively mature e-payments products, but the current adoption rate is only around 5%. The transactional ecosystem is a two-sided market, which means you have consumers and merchants – two distinct parties with distinct needs – but you need both for a transaction to be successful. For example, there's no point in a merchant providing a terminal for credit card transactions if no one has a credit card, and vice versa, which creates a kind of 'chicken and egg' situation standing in the way of adoption. The main challenge was therefore to change behaviour on both sides. Solving this challenge requires a specific approach with an understanding of the common laws of two-sided markets. At INNOPAY, we are very familiar with those laws and how to address them based on our inclusive, collaborative approach.

INNOPAY was recommended because of its unique collaborative approach to co-creation. Could you elaborate on that?

I mean that joining forces helps to overcome all kinds of challenges in two-sided markets. Our client's aim is to advance the overall growth and prosperity of the country as a whole. This also means growing the entire transactional ecosystem rather than playing a zero-sum game in which one or two dominant 'winners' take it all, which is what we're currently seeing in platform-based models. Our inclusive approach is based on setting up a scheme-based model based on mutual agreements relating to business, legal, operational, functional and technical aspects. Such a scheme provides equal access for all kinds of organisations, irrespective of their size – which is particularly relevant in a country with such a high number of smaller, local banks. This creates healthy competition based on better value propositions for end users (consumers and merchants) while growing the whole digital transaction market, creating a win-win situation for everyone. INNOPAY has a successful track record of creating and launching schemes since 2005, both in Europe and beyond. As an added benefit, this type of collaborative approach will make the banking industry more resilient against FinTech giants trying to enter the market.

What are the next steps?

The project came to an end in early February, but we're keeping in touch with the client to offer support during the execution phase as necessary. We developed a very warm relationship during the project, and it was hugely rewarding to hear the

CEO describe us as "part of their story" when we were saying our goodbyes.

Did you face any cultural issues?

The Dutch culture is less formal and hierarchical than many Asian cultures, of course; we took those differences into account, such as by holding more one-on-one meetings to build trust. We discovered that it could be just as important to listen to what people didn't say as what they did. I think that our typical Dutch bluntness worked in our favour; the client was looking for an honest and straight-talking partner in order to make real progress. We have extensive experience of collaboration and co-creation projects in various countries, and the basic principles remain the same; it's about carefully balancing stakeholder needs and interests, creating a shared purpose and guiding everyone towards the end goal by asking the right questions.

What were your personal highlights during the project?

I really enjoyed being immersed in a whole new culture for a longer period of time. But above all, this was a terrific opportunity to talk to so many high-level stakeholders from across the whole payments industry, to apply my knowledge from other markets and to gain new perspectives in this one – which will in turn help me in future projects, wherever they may be in the world!

ORIGINAL INTERVIEW

GET IN TOUCH

INTERVIEW

Why data sovereignty is the cornerstone of digital trust in the transactional era.

15 June 2020

Mariane ter Veen

Guest author:
Viivi Lähteenoja
MyData Global

Trust is the essential oil needed to make data flow in today's transactional era. However, privacy and security concerns mean that many people and organisations are increasingly unwilling to share their data. MyData Global and INNOPAY both believe that data sovereignty forms the cornerstone of digital trust. Making data sovereignty a key design principle will stimulate data sharing as the basis for enabling everyone – not just the big tech giants, but also all other businesses, organisations and especially citizens – to reap the true benefits of personal data and the transactional era. In this interview, Viivi Lähteenoja (deputy general manager at MyData Global) and Mariane ter Veen (director data sharing at INNOPAY) explain more about their efforts to help shape a positive future for the data economy.

Why did INNOPAY and MyData Global decide to join forces on the topic of data sharing?
Viivi: "MyData Global is a mission-based global nonprofit that has been facilitating a global network and organising a series of international conferences since 2016 to promote our aim – which is to create a fair, sustainable and prosperous digital society in which people are in charge of access to their data and benefit from how that data is used. When 600 people attended the first MyData conference, there was a sense of a community becoming aware of itself – that there are others out there in the world who think the same – and that idea has continued to gain traction ever since. We got to know INNOPAY through our mutual involvement in a number of projects, including

conferences on the human-centric data economy. In striving to empower people with actionable rights to complement data protection rules, our work has clear synergies with what INNOPAY is trying to achieve. We also both share a strong belief in multi-stakeholder collaboration so that everyone benefits: when one of us does well, we all do well."

Mariane: "At INNOPAY, we are indeed very closely aligned with the missions and goals of MyData Global. As an internationally active consulting firm, we're helping companies worldwide to embrace the full potential of the new transactional era. We believe this can only be done by creating a world in which data sovereignty is a key design principle – and we can convey that message more effectively if we do it jointly, which is why we are excited to be working closely with MyData Global."

What exactly is data sovereignty, and why is it so important?
Mariane: "Data sovereignty means giving people and organisations more control: to decide who has access to their data, under what conditions and for what purposes, as well as the right and possibility to revoke that access at any time. Right now, the world is undergoing a digital transformation in which every interaction is becoming a transaction: every 'like' on Facebook represents value, every purchase on an e-commerce website is preceded by numerous clicks that each involve some kind of data exchange. And with the expansion of the internet and IoT, the number of transactions is set to grow exponentially. These new kinds of values can form the basis for new business models – but society and the business world are not ready for it yet! That's why it's so important that we move away from the current 'winner takes all' thinking and create a world in which everyone – people and organisations alike – can trust the reliability, safety and security of digital transactions."

Are citizens currently aware of the topic of data sovereignty? What are people's attitudes to data and how are they changing?
Viivi: "Data has been getting some bad press recently, what with the Cambridge Analytica scandal, various data leaks and the privacy discussions around things like facial recognition and coronavirus contact tracing apps. In a way, that has been hugely beneficial in terms of raising people's awareness about how their data is used online every day. However, although this has helped to address issues around ignorance and apathy regarding personal data, the narrative all too often focuses on the things that can go wrong, and some people have become scared to share their data at all. Whereas we believe that data sharing holds huge potential for good as well. The fair use of personal data can create enormous value… for people, customers and society as a whole."

Mariane: "Exactly! Right now, consumers only seem to have a 'negative' choice: if they don't like the way their data is treated, the only option is to 'leave' the platform or to not use the service. Discussions about the way forward seem to be mainly focused on introducing more regulations rather than a positive approach. Now is the time for organisations to focus on developing solutions that offer real benefits. Just think of the possibilities of personalised medicines, for example, or how great it would be if you could easily take your connections with you if you want to switch from one social media platform to another. I also feel it's important to point out here that we don't discriminate between personal data and business-to-business or B2B data – that's an artificial distinction. Even B2B transactions inevitably involve people too, whether customers or employees. Ultimately, we both want to help companies realise that they don't have to be afraid to use personal data; they just have to transform the way they deal with it – but so far there hasn't been an effective means to do so. That's why we need to create a soft infrastructure. Only then will organisations be able to build the necessary trust so that more people become willing to share their data."

So how can organisations build the necessary trust to stimulate data sharing?
Viivi: "Showing that they use data ethically is the most beneficial way for organisations to build trust-based relationships with customers and other organisations. There's still work to be done in terms of business models, enabling regulation and legislation, technological solutions and societal attitudes, but we see steps being taken in the MyData community every day."

Mariane: "By the way, we're not talking about data ownership here. The issue isn't who owns the data, but rather who has the rights to access it and for what purpose, and that needs a soft infrastructure to facilitate it. Unlike the Industrial Revolution, which has left us dealing with the downsides such as pollution and the environmental impact around a hundred years later, we are still at the start of today's 'Data Revolution'. So we have the chance to eliminate the downsides – such as data pollution, misuse of data, the data benefit balance tilting too far in the tech giants' favour – by making data sovereignty a key design principle. This is a unique opportunity to act now and shape the future so that organisations can build competitive propositions which allow us all to reap the benefits without such problems."

Viivi: "It really is a paradigm shift that we're looking to achieve. Although no one knows exactly how the world will look in ten years' time, we share INNOPAY's conviction that we now have the opportunity to affect how things will unfold."

How do you expect the recently introduced EU Data Strategy to help accelerate the execution of the data economy?
Viivi: "MyData's thinking is very solidly rooted in the European value base and a holistic view of people as citizens, active agents with the will and capacity to make life better through the use of data. That differs from the Silicon Valley view and the platform model, where people are often seen primarily as market actors – defined by their ability to buy and sell to participate in the market."

Mariane: "And then there's the more state-led model in countries such as Russia and China: 'You can share data but we decide how'."

Viivi: "That's right. In contrast, based on European values, we take the human-centric point of view that people and data about them are not just an asset to be traded. So after many years of hard work building by countless pioneers awareness of this issue in Brussels, it was very rewarding for us to see that the recently introduced EU Data Strategy has put the human being at centre of the data about them. In fact, on page ten of the document, it explicitly mentions MyData as a promising initiative for allowing individuals to gain value from data about them and to exercise rights of control over access to their data. Therefore, we believe that the EU Data Strategy has the potential to accelerate the execution of the data economy as we would like it to be shaped."

Mariane: "In addition to supporting these important European values, the EU Data Strategy provides a boost for initiatives that are driving data sovereignty. Real-life examples such as iSHARE in the logistics sector and MedMij in healthcare already show how you can create trust by developing a soft infrastructure to give organisations and people control over the access to data. Trust is the essential oil we need to make data flow in the transactional era. That will form the foundation on top of which organisations can build competitive propositions and new business models that offer value in the future. We're seeing the emergence of a growing number of high-potential initiatives across Europe, thanks in part to support from the EU Data Strategy."

But what does all this actually mean for businesses? What can and should they do?
Viivi: "Data sharing is a very complex issue involving business, legal, technical and societal aspects. It's almost impossible for organisations to solve them alone. With nearly 90 organisation members and over 600 individual members across on six continents, the MyData community network offers access to relevant experts around the world, so organisations don't need to reinvent the wheel, as it were. We regularly work with data professionals within organisations to help them transform how they deal with personal data in order to build trust and generate value."

Mariane: "As INNOPAY, we have one clear message for organisations: You can start right now! We believe that we can no longer remain in a world of silo-based thinking and benchmarking. If you really want to reap the benefits, you have to look beyond the boundaries of your organisation and consider your whole ecosystem. Ask yourself 'What data do I need, how can I access that data in an ethical way, and how can I give customers more control in that process?'. Based on our 20 years of experience with data sharing, we've developed a 7-step approach that is already helping numerous clients to make important decisions about their data-sharing strategy every day. It covers things like internal awareness and capabilities, process optimisation and alignment in the value chain, and transparent communication to truly embed data sovereignty in the organisation. No matter what happens over the next ten years, there's no scenario in which organisations will regret making data sovereignty a key design principle so there's no reason not to do it – and they can start today!"

ORIGINAL INTERVIEW

GET IN TOUCH

INTERVIEW

‘We can only lay the foundations for the future together’

19 October 2020

Mariane ter Veen

Guest author:
Richard Tieskens
from Digiteam

INNOPAY – together with its partner Contakt – has been involved in the further digitisation of the Dutch construction sector since the beginning of this year. A lot has been achieved in terms of digitisation in recent years, but there is still plenty of work to be done. We spoke to Richard Tieskens, chairman of Digiteam, about the needs to speed up digitisation, the role of a digital scheme in that process, and Digiteam’s collaboration with INNOPAY and Contakt.

The Dutch construction sector faces several challenges. The pressure to increase construction productivity, to make existing buildings more sustainable and to participate in the energy transition is forcing more intensive collaboration within the sector. Digiteam – a sector-based initiative in conjunction with the national innovation programme for construction called ‘Bouwagenda’ – is responsible for further boosting digital collaboration in the industry. Around 37 organisations from all stages of the construction life cycle have already aligned themselves with Digiteam’s ambitions and more than 20 projects have been identified as projects that contribute to accelerating the digitisation of the sector.

“I see it as a personal mission to work together with others to help the sector move forward. Digitisation is important for the challenges that lie ahead for the sector, and – although things are already moving in the right direction – there is a real need to work in a fundamentally different way. Every organisation in the sector is working on digitisation, but they are each in their own 'bubble'. There are lots of brilliant initiatives, but they are either shared insufficiently or carried out in isolation and they are not made scalable, so the situation is still sub-optimal. If we want to advance digitisation and really make a difference, it's important to intensify digital collaboration. And that's what we're going to do with DSGO, the digital scheme that regulates access to data, which we initiated earlier this year together with INNOPAY and Contakt."

Breakthrough in data sharing

The data that organisations in the construction sector need in order to operate more efficiently and sustainably is often already available somewhere in the chain, but utilising it usually involves a lengthy and costly process. Organisations have to reach bilateral agreements each time they want to set up a new data integration, which is both time and money consuming. Since this is not always feasible at project level, opportunities for data sharing and economies of scale are often missed. Besides that, many data owners are reluctant to share data, either due to a lack of trust that chain partners will handle their data carefully or because of a fear of liability. They think that sharing their data means losing control over it.

The aim of the DSGO digital scheme is to achieve a breakthrough in digital collaboration and data sharing. Thanks to a clear set of agreements, organisations no longer have to repeatedly make their own agreements about access to data. This saves them a considerable amount of time and money. Moreover, DSGO safeguards the use of data; the agreements revolve around data owners maintaining control over their own data at all times.

"The idea for a digital scheme has been around for a long time already. After all, uniform agreements enable all supply chain partners – no matter which phase of the construction life cycle they are active in – to make easy and secure use of data that is already available somewhere. As a result, they are able to improve their mutual digital collaboration and work more efficiently and sustainably. However, financing the scheme turned out to be challenging, because no one benefits from it immediately – only in the long-term. That's why it is important for the government to support initiatives of this kind. At the same time, we also require commitment from sector organisations in terms of contributing in projects or making resources available so that the agreements can be developed."

"The next step now is to actually develop the agreements, and we will do that next year in co-creation with the sector itself. Together with INNOPAY and Contakt, we have made good progress this year and have already convinced a number of organisations to join us in this early phase. They are enthusiastic to contribute to the scheme, to a breakthrough in data sharing and to the next step in digitisation."

Unique knowledge and experience

Tieskens is very positive about the partnership with INNOPAY and Contakt, and believes that the combination of the two consultancies works well. "We have known Contakt for some time now. They know the construction sector through and through and have lots of valuable project management experience. We hadn't worked with INNOPAY before, but we were keen to do so due to their unique knowledge and experience in supporting the development of digital schemes, their collaborative approach and connecting entire ecosystems. We could put INNOPAY's core competencies to good use. Besides that, the two firms have very good 'chemistry' – they complement each other very well."

"In addition, I firmly believe that we'll get this job done successfully together. We're facing quite a challenge, so that feeling of 'togetherness' is important. The most crucial thing at the moment is to get commitment from the sector itself. We're working on making people realise that we can only advance as a sector if we pull together, and that digitisation goes beyond their own company or organisation. We're calling on everyone to collaborate on a future-proof construction sector with good reason, because we can only lay the foundations for the future together."

ORIGINAL INTERVIEW

GET IN TOUCH

INTERVIEW

Digital Sustainability is the logical extension of corporate responsibility strategies

17 November 2020

Shikko Nijland

Douwe Lycklama

"We are sleepwalking into a dystopian digital future of data pollution. If we don't act now, we risk creating a digital world which will be unfit for our children." These are the cautionary words of INNOPAY's founding partner, Douwe Lycklama, and CEO Shikko Nijland. But far from being harbingers of inevitable doom, they are bringing forward a positive message of how we can work together to assume a shared responsibility for our digital future. Just as we are collectively focusing on protecting the physical environment, so we also need to develop Digital Sustainability policies to safeguard the future wellbeing of our digital world.

Data pollution is threatening to overwhelm the transactional ecosystem

The digital age and the exponential growth in data transactions has delivered untold benefits. Transactions – such as sending someone a message, buying something in a store, booking an airline ticket online or logging on to social media – can be likened to breathing. We do it all the time without even thinking. But are we being quietly anaesthetised by the allure of these shiny baubles which apparently come without cost? Douwe and Shikko believe so: "The transactional internet delivers huge benefits but it also comes with some adverse side-effects. We describe this as 'data pollution', and we must begin viewing it through the same lens as environmental pollution. But whereas it took over 100 years to reach a crisis in the physical world, we are approaching the tipping point much faster in the digital sphere."

Data transactions are growing exponentially but there is a worrying lack of agreed governance to manage and safeguard this data. So the data becomes 'polluted' – leaking, fragmented, sometimes inaccurate and, most importantly, outside the control of the people and organisations which create the data and who are it's subjects. And this inevitably leads to a lack of trust because a handful of parties are using this data solely for their financial benefit. Now we must jointly decide on new governance models that will not only protect this data, but also rebalance the data benefits in a fairer way. And critical to that discussion is who should be responsible for the data: what will be the roles for governments, companies and individual citizens?

Shikko continues, "There is a power struggle going on for control of the internet. The balance of power is shifting away from democratically elected governments towards new internet companies which are hoarding our data. And we question whether this is a good thing. For example, consider how Google and Apple are able to dictate whether governments can access their proprietary APIs to create COVID-19 tracing programs. Do we want a limited number of huge organisations to have this level of unchecked power? We believe that power should reside with citizens, and this inevitably leads to a more decentralised data paradigm."

And this is not just an apocalyptic discussion about societal visions for the future. It also has very practical business implications for the present. With the growing amount of data scandals, we need to realign the 'data benefits balance' and put the power back in the hands of the people and organisations that create the data, or we will lose citizens' trust. This poses a real risk because a decline in trust signals a worsening relationship between businesses and their customers, as well as between governments and citizens. Less data will be shared, and less data leads to less relevance, fewer customers and diminished business success.

Welcome to this first episode of Digital Sustainability by De Nieuwe Wereld

Video: Douwe Lycklama bij De Nieuwe Wereld over digitale duurzaamheid

We believe it is now time to wake up to this problem, and collaboratively establish new governance models to safeguard our digital environment.

Digital sustainability policies are the best way to safeguard tomorrow's digital environment

The clock is ticking but Douwe is optimistic: "We can still change things if we act now. If we do nothing, then others will decide. But we are very positive that we can create a better society if we work together and put in place governance models which will support a more decentralised data future."

Central to INNOPAY's strategy is the concept of Digital Sustainability: the idea that we should focus more attention on combating the unintended negative effects of the explosion of data transactions. The cornerstone of Digital Sustainability is the development of Digital CSR policies which will safeguard the role of the people who generate the data.

Douwe continues: "The guiding principle of a Digital CSR policy must be to put the user back into the loop again. If you are a business leader or a public policy-maker, then your focus should be to put the person who is concerned with that data in control. This is called Data Sovereignty, and it concerns your customers, suppliers, employees – anyone from whom you have data. You should provide an overview of what data you have, offer them the possibility to manage that data, and to reuse their data somewhere else."

Solving this issue requires a deep understanding of the transactional ecosystem, and an openness to considering new ways of doing things. Whilst too many regulators are focusing on the symptoms of the problem (such as trying to fragment organisations like Facebook), INNOPAY proposes a different philosophy which tackles the root causes.

"We support the Open Up, not Break Up meme. Because data is a two-sided market as well; a fact mostly overlooked in any public debate about data, which mostly centres around symptom relief. Breaking up Big Tech is not the way forward. This works against interoperability, which is essential for Data Sovereignty. In the Data Sovereignty world, you know who has your data and how to re-use it elsewhere. So for example you can decide to join another social media platform without 'losing your friends'.

"Opening Up means that people are able to control their data. So we need an additional layer to the internet infrastructure – we call this a Trust (or Soft) Infrastructure. This will enable the reuse and movement of data in a secure and manageable way. In many ways the GSM infrastructure is already part of a soft infrastructure. If we change telecoms provider, we can still keep our number. The same holds true for payments and banking. You can switch banks and still be able to shop and pay your bills. So why should it be different with data? We seem to readily accept that with WhatsApp you can only call and message people within WhatsApp, while with regular GSM and SMS we would not accept this. Extending this principle to data will give us the missing soft infrastructures which will rebalance the data level playing field."

Now also available in English
'Everything Transaction' management book of 2019
Read about it in our book
Everything Transaction
Chiel Liezenberg
Douwe Lycklama
Shikko Nijland
Dutch "Management Book Of The Year" 2019

Stimulating digital sustainability requires impetus from the public and private sectors

The decentralised payments and telecoms sectors are dependent on a healthy symbiotic public/private relationship, and we now need to extend this collaboration into other domains.

"Digital Sustainability is already on the agenda of public policy-makers", says Douwe, "and we see strong signals that things are beginning to move. We believe that Europe is going to lead the way in finding this different paradigm for the digital economy and creating new regulations. Europe's 'feature' is decentralisation and federation; it's not a 'bug'."

INNOPAY's latest market research reveals that business decision-makers are also beginning to see future benefits from Digital Sustainability, and most organisations find it important to demonstrate Digital Corporate Social Responsibility as we move into the next phase of the digital era.
Shikko says: "Companies have a great opportunity to stand out if they take responsibility now, and don't wait till it's enforced. They can show their customers that Digital Sustainability is important to them. It's the same as with sustainability in the 'real' world: at first no-one did it, but then customers started demanding it. And there is also a responsibility on us as citizens to start pushing companies to develop Digital CSR policies which create a healthier digital world.

"This is not easy, but that shouldn't stop leaders from standing up and taking action. There will be a real first mover advantage in shaping the next generation digital economy based on Digital Sustainability principles. So we are urging businesses to start with something manageable. Every company can make small steps to get people thinking about Digital Sustainability. One simple example would be to make a Digital CSR policy for how you treat internal data, such as enabling employees to take their HR file with them if they move jobs. Or service your ecosystem of customers and suppliers by providing an overview and giving access to the data which you keep about them, and offering improved ways of API connectivity and standardisation."

Douwe agrees: "Our message to business leaders is this: you don't need to wait till tomorrow when everybody is doing it. Start now, take small steps, and get ahead of the game."

Visionary decision-makers are needed to take the leadership role

Digital Sustainability is a core belief within INNOPAY's 'Everything Transaction' philosophy. If we do not start tackling the problems associated with data pollution, we will not only miss out on business opportunities, but we will be responsible for creating a digital world which is every bit as polluted as the physical one.
Douwe concludes, "We are determined to spark a wave of thinking so that people become aware of this threat and can be encouraged to take practical steps to solve the problem. Even the idea that it's possible to evolve our current digital economy is something which is still undervalued. The challenges of today's digital economy are more and more understood, but there are not many solutions in sight.

"We believe there will be a small group of visionary leaders who will take up this challenge, both because they're uneasy about the way things are heading, and because they can see the commercial advantages of being the first movers in a world where companies will increasingly compete on the health of their data.

"Show all your stakeholders – including your employees and customers – that you really care, and that you see data as the next frontier of sustainability by extending your existing CSR policies into the digital realm."

INNOPAY has extensive experience of developing Digital Sustainability and Digital CSR strategies. To discuss how your organisation can take the first steps to tackling the challenges and opportunities discussed in this article, feel free to contact Douwe Lycklama and Shikko Nijland.

ORIGINAL INTERVIEW

GET IN TOUCH

PODCAST

Podcast discusses how everyone can benefit from the value of data

22 December 2020

Mariane ter Veen

In today's episode of the "Behind the click" podcast, Julia Janssen talks to INNOPAY's Mariane ter Veen. They first map out how information is currently moving on the web, and what complications are associated with it - both for the internet user and for the industry behind it. They go on to discuss data exchange in a controlled environment, data sovereignty and how everyone can benefit from the value of data.

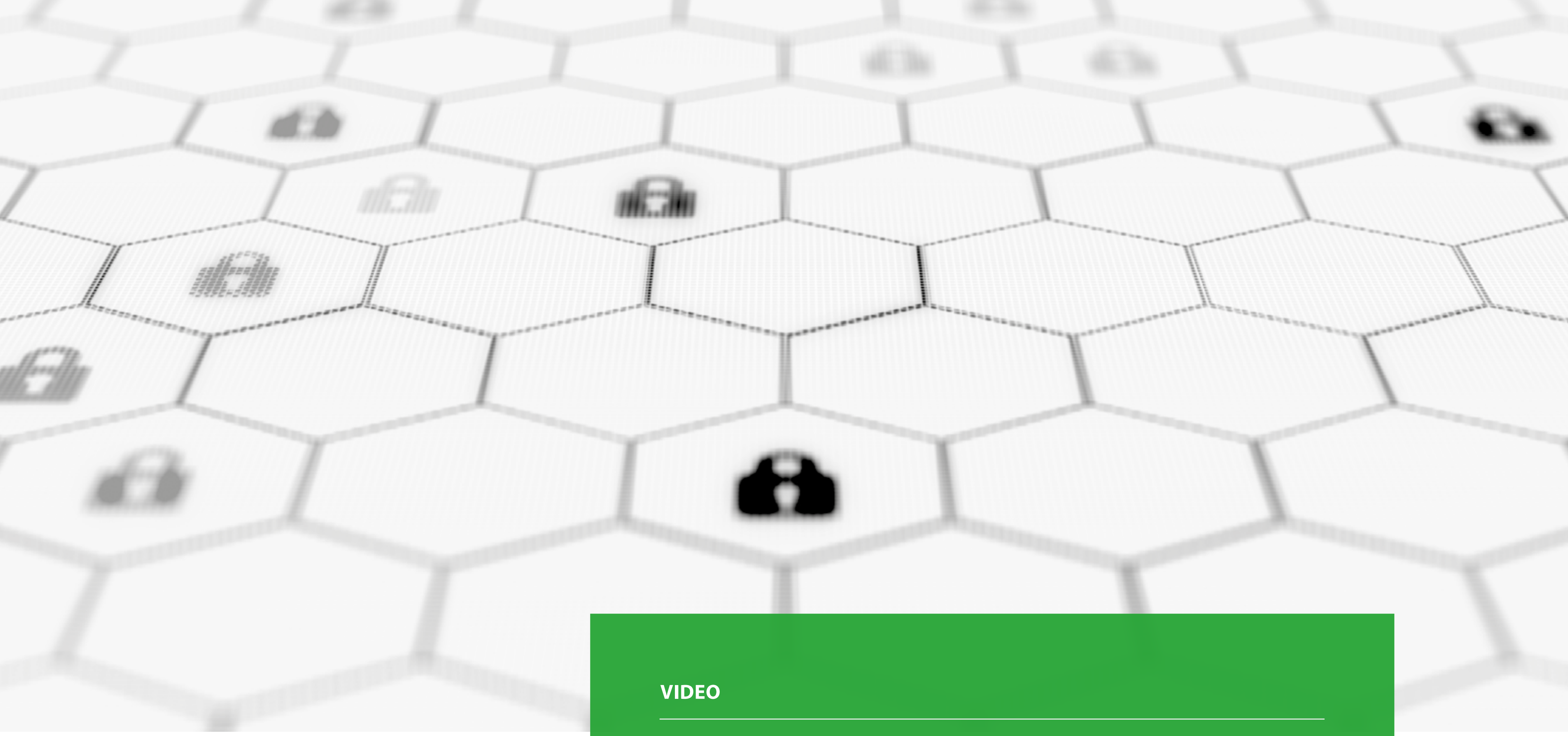
You can find the podcast episode here.

Behind the click is a series of podcasts in which Julia takes the listener on a journey behind the surface of the internet. 'What happens to the other side of the screen when you click?'. The online universe has a lot to offer. But, we hardly think about the price of admission. Nothing is free and that also applies online. When something seems free, you are the product.

Julia Janssen makes complex matters understandable and offers an innovative way of thinking for professionals. She talks to experts in the field of data ownership and data sharing, such as politicians, philosophers, lawyers and data scientists. Behind the click Podcast connects current themes (e.g. the corona app) with long-term studies.

ORIGINAL PODCAST

GET IN TOUCH



VIDEO

‘We want to make sure that European values, particular data protection issues, are fully reflected in the way we treat data’

29 April 2020

Mariane ter Veen

The European Data Strategy is built on a new approach to handling data. The EU hopes to play a leading role in the future of data security by making better decisions. INNOPAY’s Mariane ter Veen speaks in this edition of our Data Sharing Journal (#DSJ) with Yvo Volman, head of the ‘Data Policy and Innovation’ unit at the Directorate-Generale networks, Content and Technology (DG CNECT) of the European Commission.

Yvo believes that Europe can lead the way because it is strong in areas of public interest. The European Data Strategy provides a new framework for handling data, based on the belief that individuals and companies should be in control of their data. This is built around ‘European values’.

Data
Sharing
Journal

ORIGINAL VIDEO
GET IN TOUCH

VIDEO

The future relevance of banks in the data economy

8 August 2020

Mounaim Cortet

The rising importance of Open Banking, digital identity, consent management and data sharing has created a 'Blue Ocean' market for banks. We believe that they now have a unique opportunity to strengthen and truly safeguard their relevance in the data economy. But they need to start taking decisive action right now in order to demonstrate that they can provide the necessary trust to underpin new business models.

In this short video we explain our vision on digital transactions in the data economy and the implications for market actors. Get in touch if you want to know more about our vision and how you can prepare for it.

ORIGINAL VIDEO

GET IN TOUCH

VIDEO

Data Sovereignty Now Webinar: Unleashing the benefits of data in line with European values

20 October 2020

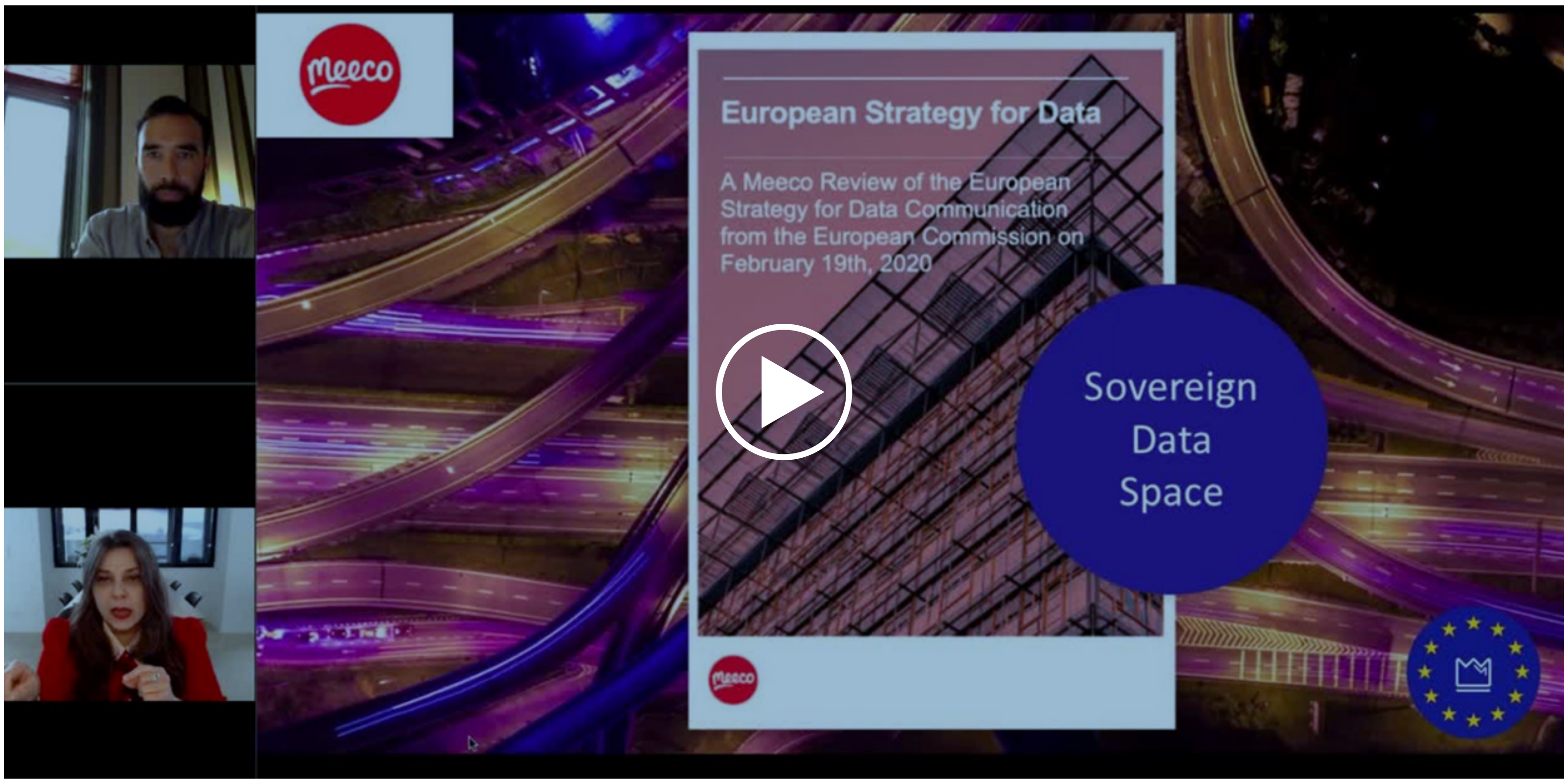
Data Sovereignty Now

On 15 October 2020, The Data Sovereignty Now movement hosted a webinar on how to unleash the benefits of data, in line with European values. If you weren't able to make it to the webinar, the recording is available below.
We want to share three key takeaways from the webinar, in the hopes that they might help you better understand the importance and meaning of data sovereignty, and how to obtain it.

Three key takeaways from our webinar about data sovereignty
We believe that the digital economy as it is known today is at risk because data is not under our direct control. We believe the only way to combat this, to release the full potential of data and build a solid and sustainable foundation for the next phase of the digital economy is to:

1. Make 'data sovereignty' the central design principle of the data economy as a whole and a prerequisite for every organisation's own data architecture.
2. Create a ('soft') infrastructure for decentralised data sharing based upon European values, built on a sound, secure and unified consent mechanism that works every entity, a person, business or government for example.
3. Focus on adoption of data sovereignty by organisations and end users, rather than prescribing necessary technology. Support businesses, governments and their IT departments / partners in offering data sovereignty functionalities to their users, based on open and well governed standards.

Do you support the mission of the Data Sovereignty Now movement and did the webinar raise your interest to become involved as a member or do you want to know more?
Let us know!



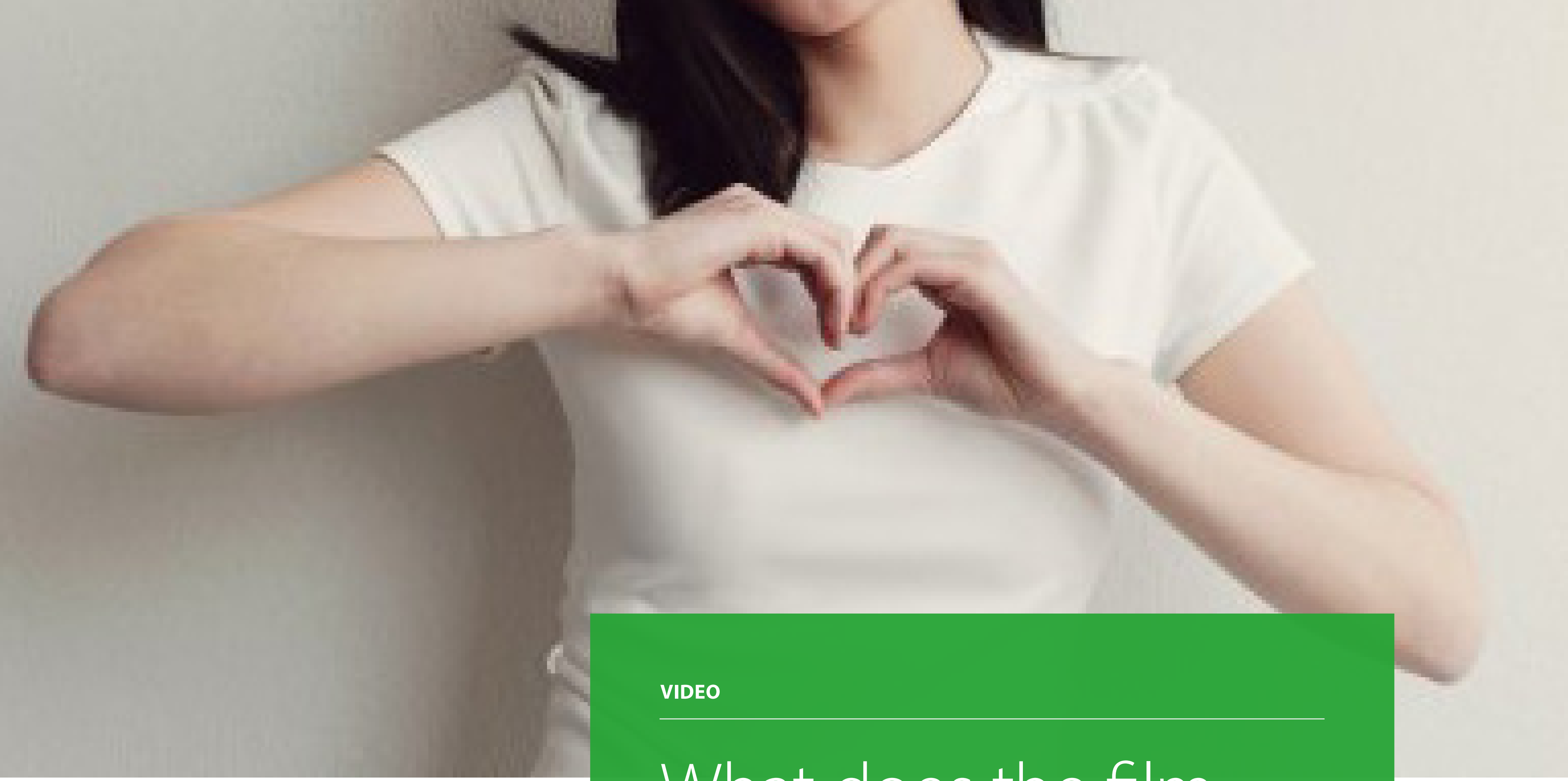
European Strategy for Data

A Meeco Review of the European Strategy for Data Communication from the European Commission on February 19th, 2020

Sovereign Data Space

ORIGINAL VIDEO

GET IN TOUCH



VIDEO

What does the film 'The Social Dilemma' teach us about digital sustainability?

8 December 2020

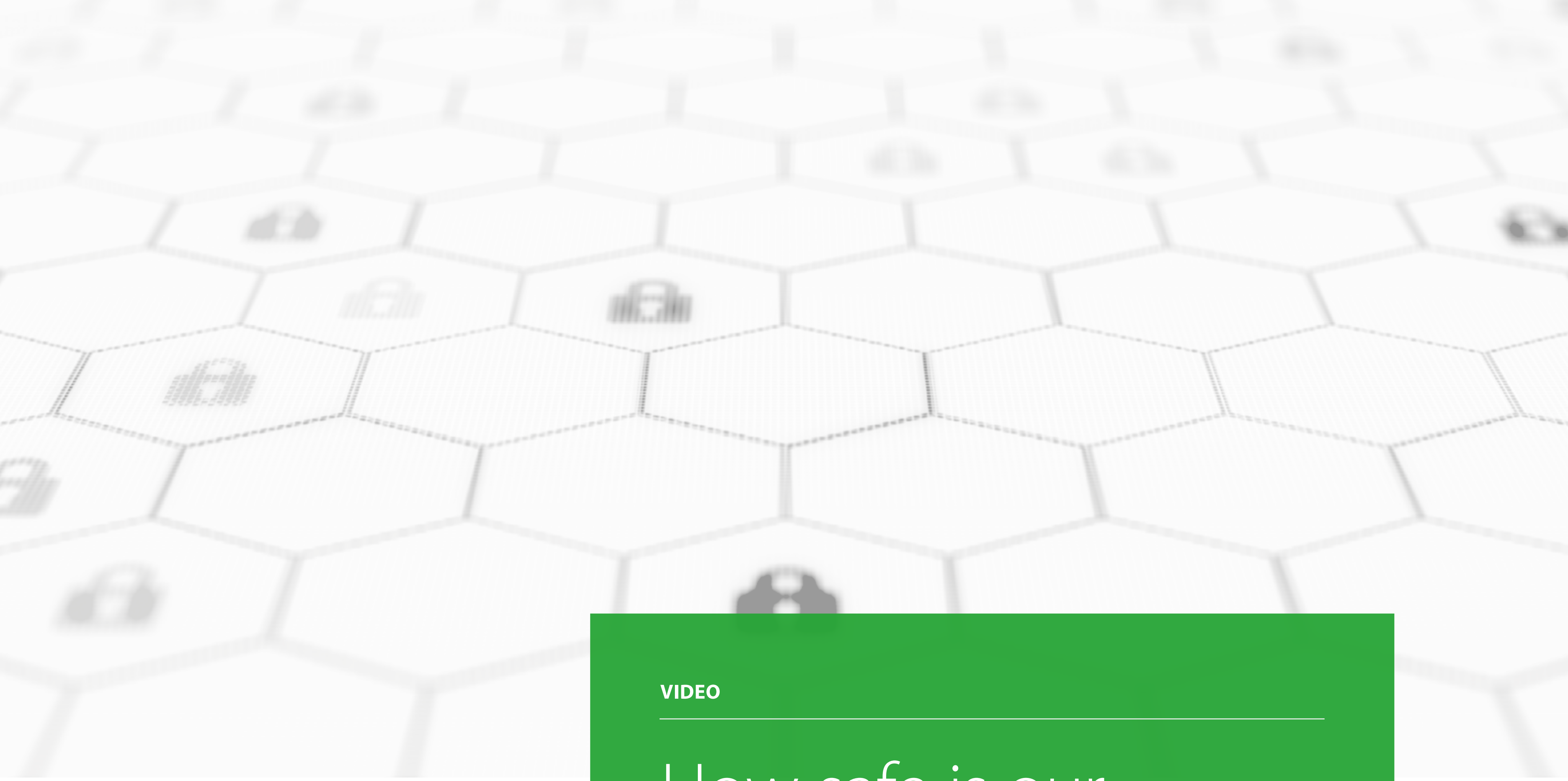
Douwe Lycklama

In this first edition of the De Nieuwe Wereld's broadcasts on Digital Sustainability, journalist and philosopher Ad Verbrugge talks to INNOPAY's Douwe Lycklama, Focco Vijselaar, Director-General for Industry and Innovation at the Dutch Ministry of Economic Affairs and Climate Change, and Marleen Stikker, founder and director of Waag. They discuss the question: "What does the film 'The Social Dilemma' teach us about digital sustainability?"

To share your views on digital sustainability, sign up for our research panel.

ORIGINAL VIDEO

GET IN TOUCH



VIDEO

How safe is our digital infrastructure? Talking about the vulnerabilities revealed by Russian hacks

26 December 2020

Data Sovereignty Now

In this second edition of the INNOPAY/De Nieuwe Wereld broadcasts on digital sustainability, journalist and philosopher Ad Verbrugge hosts a roundtable discussion with three digital security experts: Lokke Moerel (professor of global ICT at Tilburg University and member of the Dutch Cyber Security Council), Pieter Cobelens (former director of the Dutch Military Intelligence and Security Service, MIVD) and Ronald Prins (chief technology officer and co-founder of Hunt & Hackett and an expert on internet security).

The guests talk about the vulnerabilities of our digital infrastructure, the global balance of power over data, how the Dutch government can protect the data of the country's citizens and organisations, and what organisations and governments can do to protect themselves against cyberattacks.

To share your views on digital sustainability, sign up for our research panel.

ORIGINAL VIDEO

GET IN TOUCH

INNOPAY

Get in touch!

The Netherlands

Innopay BV
P.O. Box 75643
1118 ZR Amsterdam, The Netherlands
T +31 (0) 20 65 80 651

Germany

Frankfurt
c/o TechQuartier
Platz der Einheit 2
60327 Frankfurt am Main
T +49 (0)69 247538570
E info.de@innopay.com

Online

info@innopay.com
innopay.com
linkedin.com/innopay

Or stay up to date on Digital Identity, Data Sharing and Payments by subscribing to the INNOPAY Innsider!

innopay.com